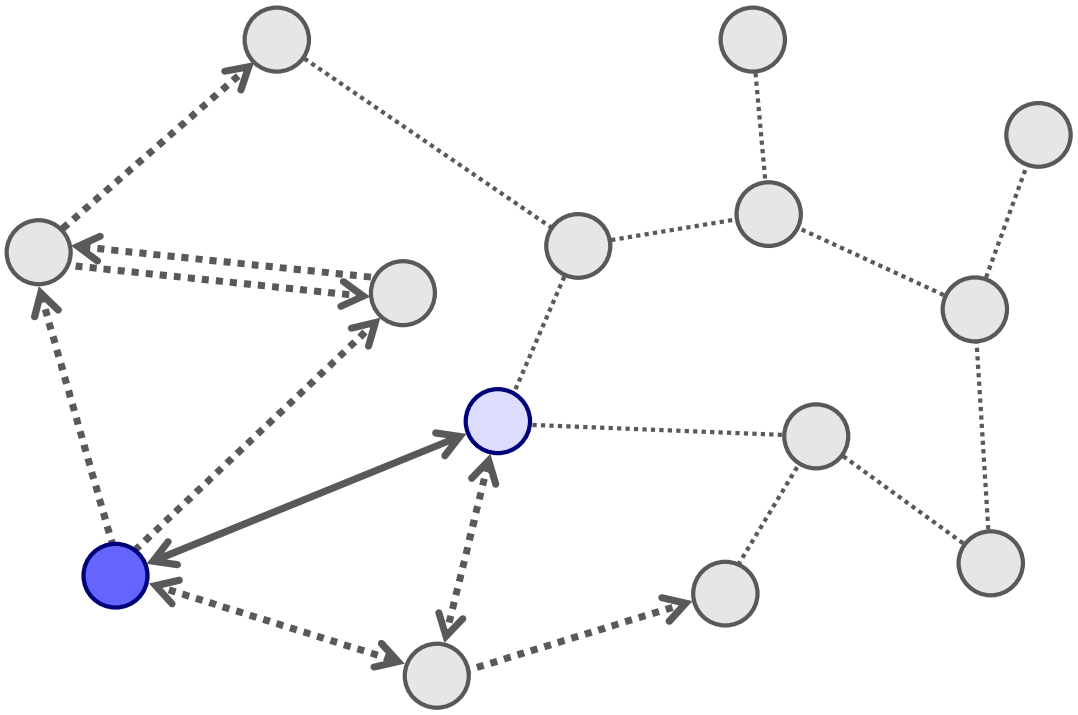
Jochen Dinger

Das Potential von Peer-to-Peer-Netzen und -Systemen

Architekturen, Robustheit und rechtliche Verortung



universitätsverlag karlsruhe

Jochen Dinger

Das Potential von Peer-to-Peer-Netzen und -Systemen

Architekturen, Robustheit und rechtliche Verortung

Das Potential von Peer-to-Peer-Netzen und -Systemen

Architekturen, Robustheit und rechtliche Verortung

von
Jochen Dinger

universitätsverlag karlsruhe

Dissertation, Universität Karlsruhe (TH)
Fakultät für Informatik, 2008

Impressum

Universitätsverlag Karlsruhe
c/o Universitätsbibliothek
Straße am Forum 2
D-76131 Karlsruhe
www.uvka.de

Universitätsverlag Karlsruhe 2009
Print on Demand

ISBN: 978-3-86644-327-3

Das Potential von Peer-to-Peer-Netzen und -Systemen – Architekturen, Robustheit und rechtliche Verortung

zur Erlangung des akademischen Grades eines

Doktors der Ingenieurwissenschaften

der Fakultät für Informatik
der Universität Fridericiana zu Karlsruhe (TH)

genehmigte

Dissertation

von

Jochen Dinger

aus Bühl (Baden)

Tag der mündlichen Prüfung:	5. Dezember 2008
Erster Gutachter:	Prof. Dr. rer.nat. Hannes Hartenstein Universität Karlsruhe (TH)
Zweite Gutachter:	Prof. Dr. iur. Thomas Dreier, M.C.J. Universität Karlsruhe (TH) Prof. Dr. rer.nat. Martin Mauve Heinrich-Heine-Universität Düsseldorf

Kurzzusammenfassung

Während die Realisierung von verteilten Systemen in den 1990er Jahren durch Client/Server-Architekturen geprägt war, kommen mittlerweile häufig auch Peer-to-Peer-Systeme (P2P-Systeme) zum Einsatz. P2P-Systeme wie BitTorrent oder Skype verfügen dabei über mehrere Millionen Teilnehmer. Verschiedene Studien zeigen auch, dass mehr als 50 % des Datenverkehrs im Internet durch P2P-Systeme verursacht wird. Davon ausgehend war es das Ziel der Arbeit, das Potential von P2P-Netzen und -Systemen für zukünftige verteilte Systeme und Netze näher zu beleuchten.

Im ersten Teil der Arbeit erfolgt daher eine umfassende Darlegung der Hintergründe und des aktuellen Entwicklungsstandes, woraus sich folgende offene Fragestellungen ergeben:

- P2P-Systeme sind für dedizierte Anwendungsbereiche mit vielen Teilnehmern gut geeignet. Weitgehend ungeklärt ist jedoch, inwieweit P2P-Techniken für komplexe verteilte Systeme wie elektronischen Marktplattformen und Systeme mit wenigen Teilnehmern geeignet sind.
- P2P-Systemen wird aufgrund der Dezentralität verbunden mit Redundanzmechanismen gemeinhin ein hoher Grad an Robustheit attestiert. Andererseits eröffnet gerade die Dezentralität neue Bedrohungspotentiale. Insofern muss die Frage beantwortet werden, welche spezifischen Angriffe existieren und welche Bedrohungen von diesen ausgehen.
- Um das Potential von P2P-Systemen zu beurteilen, muss neben technischen Aspekten eine rechtliche Einordnung vorgenommen werden, da dies gegebenenfalls Auswirkungen auf deren Gestaltung und Betrieb hat. Dabei sind im Allgemeinen weniger die vielfach untersuchten urheberrechtlichen Fragen, sondern vielmehr telekommunikationsrechtliche Aspekte von Belang.

Die Konzeption einer dienstorientierten P2P-Architektur in dieser Arbeit ermöglicht eine Diensterbringung durch mehrere Knoten auch in komplexen verteilten Systemen. Die Architektur basiert dabei auf einer Kombination von Web Services und P2P-Netzen. Insgesamt eröffnet diese Architektur P2P-Systemen somit ein wesentlich breiteres Einsatzspektrum.

Fraglich blieb bislang, ob P2P-Systeme mit wenigen Teilnehmern effizient realisierbar sind. Nachteilig dabei ist vor allem, dass für den Beitritt zu einem P2P-System, das Bootstrapping, meist zentrale Komponenten zum Einsatz kommen. Durch die kollaborative Nutzung eines weit verbreiteten P2P-Systems in Kombination mit einer dezentralen Knotensuche können diese Nachteile ausgeräumt werden. Die Tragfähigkeit der Konzepte wird durch umfangreiche empirische Messungen in der BitTorrent-DHT und entsprechende wahrscheinlichkeitstheoretischen Analysen aufgezeigt. Außerdem kann die Knotensuche durch die analytische Bewertung optimiert und ein neuartiges Verfahren vorgeschlagen werden, was die Knotensuche künftig wesentlich beschleunigt.

In Hinblick auf P2P-spezifische Angriffe erweist sich der Sybil-Angriff, bei dem ein Angreifer unter mehreren Identitäten im System agiert und somit Redundanzmechanismen aushebeln kann, als besonders schwerwiegend. In dieser Arbeit wird evaluiert, inwieweit die Ressourcenbeschränkungen eines Angreifers möglichst effektiv für die Beschränkung der Anzahl Sybils genutzt werden können. Hierzu wurde eine ressourcenbasierte Analyse anhand eines Kademlia-Netzes durchgeführt. Ferner wird der Einfluss von Sybils simulativ aufgezeigt, wobei insbesondere die katalysierende Wirkung von Routing-Table-Poisoning deutlich wird. Auf Basis dieser Analysen werden verschiedene Abwehrstrategien entworfen und bewertet. Insbesondere kann durch das neuartige Verfahren zur Selbstregistrierung die Anzahl der Knoten pro IP-Adressbereich effektiv begrenzt werden. Anhand der durchgeführten Analysen kann somit das Bedrohungspotential von Sybil-Angriffen abgeschätzt und zukünftige P2P-Systeme können unter Anwendung der aufgezeigten Abwehrstrategien robuster gestaltet werden.

Aus betrieblicher Sicht müssen neben technischen auch telekommunikationsrechtliche Aspekte bedacht werden. Die technisch-rechtliche Analyse der relevanten gesetzlichen Regelungen auf nationaler sowie europäischer Ebene zeigt, dass existierende Einordnungsschemen für P2P-Systeme ungeeignet sind. Aufgrund dessen wird ein telekommunikationsrechtliches Einordnungsschema entwickelt, durch welches die Einordnung von P2P-Systemen in den bestehenden Rechtsrahmen wesentlich erleichtert wird. Ferner werden aus dem Schema Leitlinien für Entwickler und Betreiber von Knoten abgeleitet.

Insgesamt eröffnet die vorliegende Arbeit der P2P-Technologie ein wesentlich breiteres Einsatzspektrum, indem vorhandene Verfahren und Mechanismen bewertet und in Kontext gesetzt sowie durch die Ergänzung mit neuartigen Verfahren bestehende Defizite ausgeglichen wurden. Die Bewertung der Mechanismen wurde dabei je nach Eignung durch Messungen, Simulationen und analytische Betrachtungen vorgenommen. Ferner wurden eine Reihe neuartiger Verfahren entwickelt, die zur Verbesserung von zukünftigen P2P-Systemen dienen.

Vorwort

Die vorliegende Arbeit entstand während meiner Zeit als wissenschaftlicher Mitarbeiter in der Forschungsgruppe Dezentrale Systeme und Netzdienste (DSN) am Institut für Telematik der Universität Karlsruhe (TH).

Mein besonderer Dank gebührt zunächst Herrn Prof. Dr. Hannes Hartenstein, der mir die Möglichkeit zur Promotion eröffnet hat und während der gesamten Zeit als Mentor überaus hilfreich zur Seite stand. Er lies mir dabei einerseits den – gerade in Forschung besonders wichtigen – Raum zur freien Entfaltung und förderte selbstverantwortliches Handeln. Andererseits gab er wertvolle Hinweise und Anregungen und zeigte somit zielführende Wege auf.

Ebenso möchte ich mich bei Herrn Prof. Dr. Thomas Dreier und Herrn Prof. Dr. Martin Mauve für die Übernahme des Korreferats sowie bei Herrn Prof. Dr. Ralf Reussner und Herrn Prof. Dr. Wilfried Juling für die Begleitung der mündlichen Prüfung bedanken.

Ein besonderer Dank gilt den Kollegen der Forschungsgruppe DSN, die immer motivierend und hilfsbereit zur Verfügung standen. Dabei möchte ich insbesondere den Kollegen "der ersten Stunde", Moritz Killat, Felix Schmidt-Eisenlohr und Dr. Marc Torrent Moreno danken. Sie hatten immer ein offenes Ohr für Diskussionen, lieferten zahlreiche Anregungen und haben dadurch wesentlich zum Gelingen der Arbeit beigetragen. Auch die nicht fachlichen Diskussionen sorgten dabei immer für viel Freude, auch wenn in Fußballfragen nie Einigkeit erzielt werden konnte. Ferner sei auch den Kollegen Dr. Jérôme Härri, Thorsten Höllrigl, Sebastian Labitzke, Jens Mittag und Frank Schell an dieser Stelle für ihre Kommentare, Hilfsbereitschaft und die angenehme Arbeitsatmosphäre gedankt.

Des Weiteren danke ich Herrn Prof. Dr. Wilfried Juling und Herrn Prof. Dr. Martin Gaedke, dass sie mir den Weg in die Forschung eröffnet haben, und der Forschungsgruppe von Prof. Juling, die mich in den ersten Monaten aufnahm. Ebenso gilt der Dank der Gruppe von Frau Prof. Dr. Martina Zitterbart und den Kolleginnen und Kollegen aus den Projekten SESAM und KAI. Insbesondere seien Michael Conrad, Dr. Oliver Raabe und Dr. Oliver Waldhorst erwähnt, die wichtige Impulse für die Arbeit lieferten und zu gemeinsamen Publikationen beitrugen. Den beiden letzt genannten gebührt dabei ein gesonderter Dank für die

Durchsicht des Manuskripts dieser Arbeit und entsprechende konstruktive Kritik. Dr. Raabe gilt außerdem ein besonderer Dank, da er das Interesse an der "Juristerei" in mir weckte, die nötigen Grundlagen vermittelte und essentiell zu den gemeinsamen interdisziplinären Arbeiten beitrug.

Ferner möchte ich allen Studenten für ihre wertvollen Beiträge danken. Mein besonderer Dank geht dabei an Oliver Jetter und Konrad Jünemann, die mich auf dem Weg mehrere Jahre begleiteten, herausragend unterstützten und somit wesentlich zum Gelingen der Arbeit beigetragen haben. Besonders freut mich, dass sie trotz aller Schwierigkeiten nie aufgaben und dass sie zukünftig die Forschungsgruppe DSN bereichern werden.

Weiterhin möchte ich mich bei den Kollegen aus der Technik, Herrn Detlev Meier, Herrn Gentiel Mussgnug und Herrn Frank Winter bedanken. Sie standen mir immer mit Rat und Tat zur Seite. Gleichermaßen möchte ich mich bei einer Reihe von Damen bedanken, die für mich und unsere Forschungsgruppe stets hilfsbereit zur Verfügung standen, um die zahlreichen administrativen Klippen zu umschiffen: Frau Brigitte Armbruster, Frau Ina Dvorak, Frau Astrid Hopprich, Frau Astrid Natzberg, Frau Dorothea Wagner und Frau Doris Weber.

Nicht zuletzt möchte ich meiner Frau Veronika, meinen Eltern, meinem Bruder sowie allen Freunden und Bekannten danken, die mich bei diesem Projekt stets ermuntert und unterstützt haben. Meinen Eltern Alexandra und Helmut danke ich vor allem für ihre uneingeschränkte Unterstützung, meine persönlichen Ziele verfolgen zu können. Veronika danke ich insbesondere für ihre unglaubliche Geduld und ihre auch in schwierigen Zeiten immerwährende moralische Unterstützung.

Vielen Dank!

Jochen Dinger

Bühl, im Dezember 2008

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1
Einleitung

Die Verbreitung und Nutzung von Peer-to-Peer-Systemen (P2P-Systemen) hat in den letzten Jahren immer mehr zugenommen. Verschiedene Studien zeigen, dass P2P-Systeme wie BitTorrent oder Skype über mehrere Millionen Teilnehmer verfügen (vgl. u.a. [Steiner et al. 2007]) und mehr als 50 % des Datenverkehrs im Internet verursachen (vgl. u.a. [Haßlinger 2005]). Diese Zahlen verdeutlichen die Relevanz solcher Systeme im heutigen Internet. Waren die ersten P2P-Anwendungen wie zum Beispiel Gnutella lediglich für den Dateitausch konzipiert, werden mittlerweile auch Systeme wie zum Beispiel Skype zur P2P-Internet-Telefonie oder Joost für P2P-Video-Streaming vielfach genutzt. Insofern stellt der P2P-Ansatz in einigen Bereichen eine Alternative zu der in den 1990er Jahren dominierenden Client/Server-Architektur dar.

Getreu der Maxime "Das Ganze ist mehr als die Summe seiner Teile."[1] werden P2P-Systeme aus einer Menge von Knoten, auch als Peers bezeichnet, gebildet, die miteinander kooperieren und gemeinsam ein logisches Netz bilden. P2P-Systeme zeichnen sich dabei in der Regel durch selbstorganisierende Mechanismen aus, so dass keine manuellen Eingriffe notwendig sind, um die Verbindungen zwischen den Peers zu etablieren. Daher können solche Systeme adaptiv auf veränderte Rahmenbedingungen wie Peer-Ausfälle reagieren und weisen meist eine immanente Skalierbarkeit hinsichtlich der Anzahl der Peers auf.

Obgleich die Eignung von P2P-Systemen für dedizierte Anwendungsberei-

[1] nach Aristoteles

che gegeben ist und eine intensive wissenschaftliche Untersuchung zahlreicher Aspekte bereits erfolgte, bleibt fraglich, welches Potential solche Systeme bei der Entwicklung und dem Betrieb im Allgemeinen entfalten können. Dabei erfordern insbesondere die drei folgenden Gesichtspunkte eine Klärung:

- Trotz der Vielfältigkeit von P2P-Systemen zeigt sich, dass sie in der Regel für abgegrenzte Anwendungsbereiche mit vielen Teilnehmern Verwendung finden. Weitgehend ungeklärt bleibt dabei, inwieweit P2P-Techniken im Rahmen von komplexen verteilten Systemen, wie zum Beispiel elektronischen Handelsplattformen genutzt werden können und ob P2P-Systeme mit wenigen Teilnehmern effizient betrieben werden können.

- Dezentralität verbunden mit redundanter Speicherung der Daten und alternativen Routen in P2P-Systemen führen zu einem erhöhten Robustheitsgrad hinsichtlich dem Ausfall einzelner Peers. Regelmäßig wird P2P-Systemen daher eine inhärente Robustheit attestiert. Dabei bleibt jedoch unberücksichtigt, dass sich durch die Dezentralität auch ein neues Bedrohungspotential eröffnet, da keine zentrale Authentifizierung und Autorisierung von Teilnehmern erfolgen kann. Insofern stellt sich die Frage, welche spezifischen Angriffe existieren und welches Bedrohungspotential von diesen ausgeht.

- Um verteilte Informationssysteme oder Rechnernetze rechtskonform betreiben zu können, ist eine juristische Betrachtung obligatorisch. Insofern muss neben einer technischen Würdigung auch eine rechtliche Einordnung von P2P-Systemen vorgenommen werden, da dies gegebenenfalls Auswirkungen auf deren Gestaltung und Betrieb hat. Dabei sind im Allgemeinen weniger die vielfach untersuchten urheberrechtlichen Fragen von Belang, sondern vielmehr eine telekommunikationsrechtliche Verortung, um beurteilen zu können, welche Rechte und Pflichten für Peer-Betreiber resultieren.

1.1 Zielsetzung und Beiträge der Arbeit

In der vorliegenden Arbeit wird das Potential von P2P-Systemen und -Netzen aufgezeigt. Zunächst werden dazu bestehende Systeme sowie Netze bewertet und charakteristische Eigenschaften abgeleitet. In der Folge findet eine differenzierte Analyse der Defizite bestehender P2P-Systeme in Hinblick auf die im vorigen Abschnitt genannten Aspekte statt. Hierzu werden geeignete Klassifikationsschemata und Bewertungsmodelle entwickelt. Schließlich kann durch neuartige Lösungsansätze und die vorgenommene Bewertung das Einsatzspektrum von P2P-

Systemen maßgeblich erweitert und die betrieblichen Randbedingungen können dargelegt werden. Die Arbeit ist dabei insbesondere durch folgende Beiträge gekennzeichnet:

Charakterisierung von P2P-Systemen und -Netzen: Um eine Charakterisierung von P2P-Systemen vorzunehmen, wird zunächst eine umfassende Literaturrecherche sowie eine Einordnung in den historischen Kontext vorgenommen. Daraus folgend wird eine Definition eines P2P-Systems sowie ein P2P-Ebenenmodell abgeleitet. Durch das Ebenenmodell werden insbesondere die Begriffe P2P-System, P2P-Netz und P2P-Gemeinschaft in Beziehung zueinander gesetzt werden. Des Weiteren werden die Kernelemente von P2P-Systemen identifiziert und in den Rahmen der verteilten Systeme und Rechnernetze eingeordnet. Durch Analyse der Charakteristika und faktischer Maßstäbe wie dem Verbreitungsgrad werden letztlich auch Defizite deutlich, die im Folgenden einer vertieften Betrachtung unterzogen werden.

Dienstorientierte P2P-Architektur: P2P-Systeme werden meist monolithisch für abgegrenzte Anwendungsbereiche entwickelt. In dieser Arbeit wird eine neuartige integrierte Architektur vorgestellt, welche P2P-Netze mit den Konzepten einer dienstorientierten Architektur verbindet. Durch diese Architektur lassen sich die Vorzüge von P2P-Systemen auch bei der Entwicklung von komplexen verteilten Systemen wie einer elektronischen Handelsplattform nutzen, indem Anwendungsdienste vom P2P-Netz entkoppelt werden. Somit kann die Diensterbringung durch das Zusammenwirken mehrerer Peers erfolgen. Den Dienstentwicklern stehen die P2P-Netze dabei als Module zur Verfügung. Die Architektur erlaubt insbesondere auch den parallelen Einsatz mehrerer P2P-Netze und somit die Auswahl des P2P-Netzes je nach Dienstanforderungen.

Dezentrales Bootstrapping für Mikro-P2P-Systeme: Systeme mit einer geringen Teilnehmerzahl können vom P2P-Ansatz in der Regel weniger profitieren, da hierbei die Skalierbarkeit von P2P-Systemen hinsichtlich der Teilnehmer nicht zum Tragen kommt und für den Aufbau bzw. Beitritt (engl. Bootstrapping) in der Regel ein wohlbekannter, d.h. zentraler, Bootstrap-Server eingesetzt wird. In der Arbeit wurde eine kollaborative Architektur präsentiert, die ein dezentrales Bootstrapping von so genannten Mikro-P2P-Systemen mittels eines weit verbreiteten P2P-Systems wie BitTorrent ermöglicht. Um die Anwendbarkeit des Ansatzes zu demonstrieren, wurde in einer umfangreichen empirischen Studie gezeigt, dass BitTorrent hierfür geeignet ist. Die dabei entwickelte Methodik und Modelle können wiederum bei der Analyse weiterer P2P-Systeme Verwendung finden.

Ferner konnte die Suche nach Peers mittels eines analytischen Modells optimiert werden und es wurde ein Verfahren entwickelt, durch welches die Wahrscheinlichkeit ein Knoten zu finden in zukünftigen P2P-Systemen wesentlich gesteigert werden kann.

Evaluierung der Gefahr von Sybil-Angriffen und Entwurf adäquater Abwehrstrategien: Bei P2P-Systemen erweisen sich insbesondere die Dezentralität und Redundanz in Verbindung mit selbstorganisierenden Mechanismen als vorteilhaft, da hierdurch eine Robustheit gegenüber Ausfällen einzelner Peers sichergestellt werden kann. Dabei bleibt zu beachten, dass hierdurch nicht zwangsläufig eine Resistenz gegen P2P-spezifischen Angriffe erreicht wird. Bei näherer Betrachtung erweist sich vor allem der so genannte Sybil-Angriff als äußerst effektiv, durch welchen ein böswilliger Teilnehmer unter sehr vielen Identitäten am System teilnehmen und somit auch die meist redundanzbasierten Robustheitsmechanismen aushebeln kann. Im Rahmen der Arbeit wird mittels einer ressourcenbasierten Analyse dargelegt, welches Bedrohungspotential solche Angriffe eröffnen. Ferner werden Abwehrstrategien wie das so genannte Selbstregistrierungsverfahren entwickelt und deren Wirksamkeit dargelegt, durch welche der Einfluss von Angreifern erheblich reduziert und die Bedrohung durch Sybil-Angriffe somit wesentlich verringert wird.

Telekommunikationsrechtliches Einordnungsschema und Leitlinien für Entwickler und Betreiber: Im Rahmen einer technisch-rechtlichen Analyse werden die relevanten rechtlichen Normen identifiziert, wobei insbesondere auch der europäische Rechtsrahmen gewürdigt wird. Bestehende Einordnungsschemata erweisen sich dabei in Bezug auf neue Technologien wie P2P-Systeme als nicht tragfähig, da die Technologieneutralität nicht gewahrt wird. Insofern erfolgt die Entwicklung eines neuen Klassifikationsschemas, durch welches die Einordnung von P2P-Systemen in den Rechtsrahmen wesentlich erleichtert wird und welches die juristischen Kriterien in Einklang mit den fachwissenschaftlichen Aspekten bringt. Die daraus resultierenden Rechtsfolgen werden ermittelt und eine Bewertung dieser in Form von entsprechenden Leitlinien für Entwickler und Betreiber vorgenommen.

Teile dieser Arbeit wurden bereits in [Conrad et al. 2005a], [Conrad et al. 2005b], [Jünemann & Dinger 2008], [Dinger & Hartenstein 2005], [Dinger et al. 2008], [Dinger & Hartenstein 2006a], [Dinger & Hartenstein 2006b], [Dinger et al. 2006], [Raabe et al. 2007], [Raabe & Dinger 2007], und [Dinger & Hartenstein 2008] veröffentlicht.

1.2 Gliederung der Arbeit

Die Arbeit gliedert sich in folgende Teile:

In Kapitel 2 wird eine Taxonomie eingeführt, welche insbesondere die Definition eines P2P-Systems beinhaltet. Hierzu wird auch in die Historie solcher Systeme eingeführt und eine Abgrenzung der Begrifflichkeiten vorgenommen. Abschließend werden ausgewählte Systeme sowie Netze präsentiert und eine Übersicht relevanter Arbeiten gegeben. Die Charakterisierung von P2P-Systemen wird in Kapitel 3 vorgenommen. Aus dieser leitet sich anschließend die konkretisierte Zielsetzung der Arbeit ab.

In Kapitel 4 wird eine dienstorientierte P2P-Architektur präsentiert, durch welche sich P2P-Techniken auch in komplexen Anwendungsbereichen wie einem elektronischen Marktplatz nutzen lassen. Ferner wird durch eine empirische Studie verdeutlicht, wie ein Aufbau von Mikro-P2P-Systemen ohne zentrale Komponenten möglich ist. Das Bedrohungspotential durch Sybil-Angriffe und entsprechende Abwehrstrategien wird vertieft in Kapitel 5 betrachtet. Abschließend wird in Kapitel 6 die aus betrieblicher Sicht essentielle, telekommunikationsrechtliche Verortung vorgenommen, ohne welche keine Beurteilung der Rechte und Pflichten von Peer-Betreibern stattfinden kann.

Die Arbeit schließt in Kapitel 7 mit einer Zusammenfassung der Ergebnisse und einem Ausblick auf weiterführende Arbeiten.

2

P2P-Netze, -Systeme und -Anwendungen

Ziel dieses Kapitels ist es, die Grundlagen darzulegen, die für die Bewertung des Potentials von P2P-Systemen und somit für das Verständnis der Arbeit nötig sind. Ausgehend von der Historie wird eine Definition des Begriffs P2P-System sowie eine Einordnung weiterer Begriffe wie P2P-Netz in einem Ebenenmodell vorgenommen. Des Weiteren erfolgt eine Abgrenzung zu anderen Themengebieten wie Ad-hoc-Netzwerken und Grids. Im zweiten Teil des Kapitels werden ausgewählte P2P-Systeme und -Netze sowie weitere zusammenfassende Arbeiten vorgestellt, um einen Überblick, aber auch Einblick in die konkrete Ausgestaltung von Systemen zu geben. Abschließend erfolgt eine Bewertung der vorgestellten Mechanismen.

2.1 Hintergrund

Um das Potential von P2P-Systemen und -Netzen zu erkennen, ist es unerlässlich, die Hintergründe zu beleuchten, die zur Entwicklung derselben geführt haben. Dabei spielt die Evolution des Internet eine entscheidende Rolle, die wiederum stark durch die Evolution verteilter Informationssysteme beeinflusst war. Insofern erfolgt die Betrachtung der Hintergründe zum einen aus Sicht von Informationssystemen im Internet. Zum anderen werden die Veränderungen im Internet

und die damit einhergehenden Herausforderungen aus Sicht des Netzes bzw. der Netzwerkprotokolle dargestellt.

2.1.1 Evolution des Internet – aus Sicht von Informationssystemen

Im Vergleich zu den Anfängen hatte sich das Internet Ende der 1990er Jahre merklich verändert. Zu Beginn des Internet in den 1970er Jahren dominierten Großrechner (engl. Mainframe) die Szenerie. Die Informationsverarbeitung fand zentralisiert auf diesen Großrechnersystemen statt und die Nutzer waren über so genannte Terminals, welche lediglich Zeichen auf einem Monitor darstellten, mit dem Rechner verbunden. Sämtliche Berechnungen so auch die Anordnung der Zeichen fand dabei zentral statt (vgl. auch Tier-1-Architektur in Abschnitt 4.1.2). Der Fokus des Internet lag daher auf der Vernetzung von großen Rechnersystemen [Leiner et al. 2003].

Die Großrechner verschiedener Standorte waren teilweise bereits durch unterschiedliche Netze verbunden, so dass das Ziel des Internet letztlich darin bestand, ein Netz und insbesondere eine Protokollfamilie[1] zu schaffen, die es ermöglichte unterschiedliche Netze miteinander zu verbinden. Solche Großrechnersysteme zeichneten sich dadurch aus, dass sie an einen festen Standort gebunden und, soweit keine Fehler auftraten, immer verfügbar waren. Aus Sicht des Internet war insofern eine gleichbleibende IP-Adresse vorgesehen, die fest einem System zugeordnet werden kann.

In den 1980er Jahre nahm die Verbreitung von lokalen Netzwerken wie Ethernet und PCs zu. Dadurch konnte eine Aufteilung der Aufgaben erfolgen und das Client/Server-Architekturprinzip konnte somit auf Rechnerebene implementiert werden (vgl. auch Tier-2-Architektur in Abschnitt 4.1.2). Dies unterscheidet sich von den Anfängen des Internet, als Rechner sowohl als Server als auch Client genutzt wurden und das Client/Server-Paradigma nur auf Ebene von Softwareprozessen zum Tragen kam. In den 1990er Jahren entwickelte sich die Client/Server-Architektur auf Rechnerebene schließlich zum dominierenden Architekturmuster [Alonso et al. 2004, S. 13]. Aus Sicht des Netzwerks sind Rechner, die als Server fungieren, wie Mainframes auch, durch einen auf ständige Verfügbarkeit angelegten, stationären Betrieb gekennzeichnet. Client-Rechner hingegen sind typischerweise nur temporär in Betrieb und werden teilweise auch mobil oder zumindest nomadisch, d.h. an wechselnden Standorten, betrieben (vgl. auch [Kleinrock 1995]).

[1] Die Protokollfamilie, welche dem Internet zugrunde liegt, wird in der Regel kurz mit TCP/IP bezeichnet, da diese beiden Protokolle die Kernelemente des Internet-Protokollstapels bilden (vgl. [Clark 1988]).

Der zunehmende Erfolg und die beginnende Kommerzialisierung des Internet Mitte der 1990er Jahre [Kurose & Ross 2004, S. 56 ff] führte dazu, dass auch Client-Rechnern, die vormals nur in lokalen Netzen betrieben wurden, ein Zugang zum Internet eröffnet wurde. Darüber hinaus erwuchs das Bedürfnis vormals autonom betriebene PCs mit dem Internet zu verbinden. Insofern änderten sich auch die Rahmenbedingungen für das Internet. Ein Teil der Rechner, die Clients, waren im Gegensatz zu Servern nicht mehr ständig mit dem Internet verbunden, sondern wählten sich bspw. per Modem temporär ein (vgl. u.a. [Minar & Hedlund 2001, S. 8 ff]). Da diese Rechner nur auf Informationssysteme, die Server, zugriffen, benötigten sie keine langfristig gleichbleibende und wohlbekannte IP-Adressen.

Daher wurden verschiedene Verfahren wie das Point-to-Point Protocol (PPP) oder das Dynamic Host Configuration Protocol (DHCP) entwickelt, mittels derer eine dynamische Zuweisung von IP-Adressen möglich ist. Darüber hinaus eröffnen so genannte Network Address Translation-(NAT-)Verfahren die Möglichkeit, mehrere Endsysteme hinter einer öffentlichen IP-Adresse zu verbergen (vgl. u.a. [Peterson & Davie 2003, S. 328]). Beim Einsatz solcher Techniken ist jedoch die *langfristige* Erreichbarkeit und eindeutige Adressierbarkeit von Clients auf Basis von IP-Adressen nicht mehr gegeben und somit kann kein direkter Verbindungsaufbau hin zum Client erfolgen.

Server zeichnen sich im Vergleich zu Clients zum einen durch ihre Eigenschaft als Dienstgeber aus, indem sie Ressourcen bereitstellen. Zum anderen verfügen Server aber auch über eine gleichbleibende Adresse, zu welcher sich die Clients verbinden können, und dienen somit als zentraler Koordinationspunkt für die Clients.

Insbesondere gegen Ende der 1990er Jahre nahmen die verfügbaren Ressourcen wie Bandbreite[2], Rechenleistung und Speicherplatz der Clients deutlich zu. Aus Sicht der Informationssysteme entstand somit eine grundlegende Motivation für P2P-Systeme, nämlich die teilweise brachliegenden Ressourcen der Clients zu nutzen, um Ressourcen auf Seiten des Servers einzusparen, unter der Randbedingung der teilweise eingeschränkten Erreichbarkeit von Clients.

2.1.2 Evolution des Internet – aus Netzsicht

Laut D. Clark et al. werden aufgrund von veränderten Rahmenbedingungen neue Konzepte, Architekturen und Protokolle für das Internet benötigt [Clark et al. 2005]. Vor allem die grundlegende Annahme, ein System im Internet verfügt

[2] Bandbreite wird in dieser Arbeit nicht im Sinne der Breite eines Frequenzbandes, sondern als maximale Datenübertragungsrate eines Kommunikationskanals verstanden (im Sinne von [Peterson & Davie 2003, S. 40 ff]).

über *eine* dauerhaft gleichbleibende, statische IP-Adresse, ist nicht mehr uneingeschränkt zutreffend. Solche Systeme können zwar selbst im Internet aktiv werden. Es ist aber nicht ohne weiteres möglich, die Systeme zu kontaktieren, wie es bspw. für den Aufbau einer Sprachverbindung notwendig ist. So stellt sich insbesondere die Frage wie Systeme, denen dynamisch eine IP-Adresse zugeteilt wurde, dauerhaft und eindeutig adressiert werden können.

Das Internet entstand im Kontext eines Forschungsprojekts der DARPA[3] und stellte insbesondere auch eine Plattform für Wissenschaftler bereit, um neue Netzwerkprotokolle zu testen. Durch den hohen Verbreitungs- und Nutzungsgrad des Internet sind mittlerweile jedoch Änderungen im Netz kaum noch bzw. nur sehr langsam möglich. Dies zeigt sich unter anderem bei Protokollen wie Mobile-IP oder IPv6[4] (vgl. u.a. [Peterson & Davie 2003, S. 295, 328]), mittels derer die oben genannten Probleme (zumindest in Teilen) gelöst werden können, die bisher aber kaum bzw. nur schleppend Verbreitung gefunden haben.

Insofern bestand aus Netzsicht das Bedürfnis, neue Protokolle ohne Änderung des Kernnetzes und der grundlegenden Protokolle realisieren zu können. In den letzten Jahren erlangten zur Lösung dieses Konfliktes so genannte *Overlay-Netze* zunehmend Relevanz [Peterson & Davie 2003, S. 680]. Overlay-Netze spannen ein logisches Netz[5] über einem oder mehreren bestehenden Basisnetzen auf und erlauben so die Implementierung neuer Funktionalitäten ohne Eingriff in die bestehende Infrastruktur.

Ein Beispiel solcher Overlay-Netze stellen virtuelle private Netze (engl. Virtual Private Network, VPN) dar, mit deren Hilfe interne Netzwerke gesichert über das Internet miteinander verbunden werden können. Ein weiteres Beispiel sind Multicast-Protokolle, die auf IP-Ebene keine globale Verbreitung gefunden haben, auf Anwendungsebene mittels eines Overlay-Netzes jedoch häufig zur Anwendung kommen. Dabei sei angemerkt, dass das Internet selbst nur als logisches Netz konzipiert war, um Netze zu verbinden und eine Ende-zu-Ende Verbindung über Netzgrenzen hinweg zu ermöglichen [Peterson & Davie 2003, S. 680 ff].

Aus Netzsicht ergab sich somit eine grundlegende Motivation für P2P-Netze, nämlich neben der Adressierbarkeit von Clients adaptive Overlay-Netze zu schaffen, die sich ändernden Umgebungsbedingungen anpassen und keinen Eingriff in die Netzinfrastruktur nötig machen.

[3] Defense Advanced Research Projects Agency des Verteidigungsministeriums der Vereinigten Staaten

[4] Aufgrund der zunehmenden Adressknappheit bei IPv4 wird die Verbreitung von IPv6 in den nächsten Jahren aller Voraussicht nach stark zunehmen, dennoch erweist sich der Prozess der Umstellung als sehr langwierig.

[5] *Logische Netze* werden auch als *virtuelle Netze* bezeichnet.

2.2 Historie von P2P-Systemen

Der Begriff *Peer-to-Peer (P2P)* bzw. *P2P-System* wurde Ende der 1990er Jahre vor allem durch den immensen Erfolg der Musiktauschbörse *Napster* geprägt.

> *"Peer-to-peer 'year zero' can effectively be set to Napster."*
> von J. Crowcroft und I. Pratt [Crowcroft & Pratt 2002]

Verschiedene Autoren weisen jedoch zurecht daraufhin, dass es bereits vor Napster P2P-ähnliche Systeme gab (vgl. u.a. [Crowcroft & Pratt 2002], [Shirky 2001]). Im weitesten Sinne entspricht auch der Versand von E-Mails dem P2P-Paradigma [Shirky 2001]. Auch bei Routing-Protokollen[6] wie OSPF oder BGP handelt es sich letztlich um P2P-Protokolle [Crowcroft & Pratt 2002]. Darüber hinaus fand der Begriff Peer-to-Peer vor Napster bereits beim Netzwerkmanagement Verwendung (vgl. u.a. [Fairley 1990] und [Simon 1991]). Des Weiteren weisen zahlreiche wissenschaftliche Arbeiten und Systeme, wie zum Beispiel der *Eternity*-Dienst [Anderson 1996] aus dem Jahr 1996 P2P-typische Merkmale auf. Diese wurden aber (zunächst) nicht als P2P-Systeme bezeichnet. Auch die Arbeit von Plaxton et al. [Plaxton et al. 1997], welche als Grundlage für viele P2P-Netze (vgl. Abschnitt 2.4.3) dient, wurde bereits 1997 veröffentlicht.

Dennoch stimmen die oben genannten Autoren überein, dass es sich bei Napster um das erste P2P-System handelt, obwohl Napster paradoxerweise im Sinne üblicher Definitionen nur in Teilen ein P2P-System darstellt (vgl. Abschnitt 2.3.1).

2.2.1 Die erste Generation von P2P-Systemen

Das vermeintlich erste P2P-System, Napster, wurde von Shawn Fanning entwickelt und im Mai 1999 der Öffentlichkeit präsentiert. Bei Napster handelte es sich um eine so genannte *Dateitauschbörse*, bei welcher die Teilnehmer Dateien, im Fall von Napster hauptsächlich Musikstücke, untereinander austauschen konnten. Das System bestand aus zwei Komponenten: einem zentralen Verzeichnis[7], das von Shawn Fannings Firma Napster Inc. betrieben wurde, und einer P2P-Anwendung, welche den Teilnehmern zur Verfügung gestellt wurde. Die P2P-Anwendung wurde teilweise auch als *Servent* bezeichnet, um die Mischung aus Client- und Server-Funktionalität deutlich zu machen. In Abb. 2.1 ist die Architektur des Systems skizziert.

Die Peers teilen dabei die von ihnen angebotenen Musikdateien dem zentralen Verzeichnis mit. Wird eine Datei gesucht, stellt der suchende Knoten[8] eine entsprechende Suchanfrage an das Verzeichnis und bekommt im Erfolgsfalle eine

[6] vgl. zu Routing-Protokollen u.a. [Peterson & Davie 2003, S. 282 ff bzw. S. 308 ff]
[7] auch als Index bezeichnet
[8] Die Begriff Peer und Knoten werden in dieser Arbeit synonym verwendet.

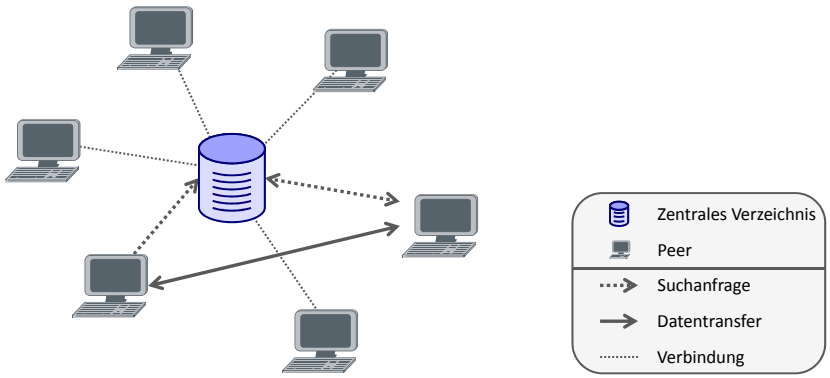


Abbildung 2.1: Aufbau des P2P-Systems Napster

Liste von Peers zurück, welche die Datei anbieten. Der folgende Dateiaustausch findet zwischen den Peers direkt, *Peer-to-Peer*, statt, ohne dass das zentrale Verzeichnis involviert ist. Insofern handelt es sich bei Napster nicht um eine komplett dezentrale Architektur, sondern um eine Mischform, die im Folgenden als *hybride Architektur* bezeichnet wird (vgl. Abschnitt 2.4.1).

Aus technischer Sicht stellte vor allem das zentrale Verzeichnis sowohl hinsichtlich der Skalierbarkeit als auch der Robustheit eine Schwachstelle dar. Außerdem entstand durch diese zentrale Komponente eine organisatorische Zentralisierung des Systems, da das Verzeichnis einen Betreiber, die Firma Napster Inc., hatte. Insofern gab es *einen* Angriffspunkt für sicherheitstechnische, aber auch politische, rechtliche und ökonomische Attacken [Crowcroft & Pratt 2002, S. 4].

Die Musikindustrie versuchte sehr schnell eine Schließung des Systems zu erreichen, da über das System vielfach urheberrechtlich geschützte Musikstücke getauscht wurden. Dabei wurde Napster letztlich der zentrale Anker zum Verhängnis. Die Firma Napster Inc. stellte sich zwar auf den Standpunkt, dass das Verzeichnis, einer Suchmaschine vergleichbar, nur Informationen bereitstellt, wo welche Inhalte zu finden sind. Die Richterin M. Patel teilte diesen Standpunkt jedoch nicht, so dass durch die Musikindustrie im Juli 2000 eine einstweilige Verfügung gegen Napster erwirkt werden konnte [Richtel 2000]. Durch Anrufung eines Berufungsgerichts konnte anschließend die Schließung vorübergehend abgewendet werden. Trotzdem sah sich Napster nach wie vor einer Flut von gerichtlichen Auseinandersetzungen ausgesetzt. Diese rechtlichen Auseinandersetzung nahmen erst ein Ende als Bertelsmann im Oktober 2000 überraschenderweise Napster übernommen hat. Dabei war es die Intention von Bertelsmann, zum einen den Erfolg und Bekanntheitsgrad der Tauschbörse zu nutzen und zum anderen Napster so umzugestalten, dass ein rechtskonformer Austausch bzw. Bereitstellung von Musikdateien stattfinden konnte. Die Ausführungen in dieser Arbeit und (den meisten) anderen Arbeiten zur Architektur von Napster beziehen

sich auf Napster wie es zwischen 1999 und 2001 funktionierte und weicht insofern von der Funktionsweise des heutigen Napster ab. Die Architektur des aktuellen Napster-Systems ist weitestgehend unbekannt, da es sich mittlerweile um ein geschlossenes rein kommerzielles System handelt.

Als Reaktion auf die drohende Schließung von Napster wurde das P2P-Protokoll *Gnutella* entwickelt, welches im März 2000 zunächst in Form einer Applikation veröffentlicht wurde (vgl. u.a. [Röttgers 2003, S. 24]). Im weiteren Verlauf entstanden dann weitere P2P-Anwendungen, welche das Protokoll implementierten. Zielsetzung von Gnutella, wie bei Napster auch, bestand darin, Dateien zwischen Peers auszutauschen. Im Gegensatz zu Napster wurde jedoch auf zentrale Komponenten verzichtet, so dass dieser Angriffspunkt entfiel.

Die erste Version des Gnutella-Protokolls, die als *Gnutella 0.4* bezeichnet wird, ist sehr einfach aufgebaut. Jeder Knoten pflegt eine Tabelle mit anderen bekannten Knoten und leitet Suchanfragen an all diese bekannten Knoten weiter. Insofern wird diese Art der Weiterleitung auch als Fluten bezeichnet. Das Fluten wird zwar durch verschiedene Mechanismen wie einen Time-To-Live-Zähler beschränkt (vgl. hierzu Abschnitt 2.4.2), dennoch erwies sich die erste Version von Gnutella als nicht skalierbar [Lv et al. 2002]. Als im Juli 2000 die Schließung von Napster drohte, offenbarte sich dieses Skalierungsproblem auch. Nachdem sehr viele Nutzer von Napster zu Gnutella überschwenkten, auch als "Napster Flood" bezeichnet [Sripanidkulchai 2001], wurde Gnutella mit Suchanfragen überflutet, so dass die Verfügbarkeit bzw. Leistung stark beeinträchtigt war [Pavlov & Saeed 2004].

Die Reduktion der Nachrichtenanzahl war das Hauptziel bei der Weiterentwicklung von Gnutella. In der folgenden Version *Gnutella 0.6* [Klingberg & Manfredi] wurden die Knoten daher in einer Hierarchie organisiert und in so genannte Superpeers[9] und Leafs unterteilt. Ein Leaf unterhält dabei in der Regel nur zu *einem* Superpeer eine Verbindung und das Superpeer agiert wiederum als eine Art Proxy. Das Superpeer leitet insbesondere Suchanfragen nur an solche Knoten weiter, welche die gesuchte Datei haben, so dass sich letztendlich die Anzahl der Nachrichten deutlich reduziert. Dieses Konzept wird auch als *Superpeer*-Architektur bezeichnet [Chawathe et al. 2003] und in Abschnitt 2.4.2 näher erläutert. In der Folge wurde diese Superpeer-Architektur auch von weiteren Anwendungen wie zum Beispiel der Dateitauschbörse Kazaa genutzt. Auch das weit verbreitete P2P-System *Skype* [WWW Skype], das vor allem zur Sprachtelefonie genutzt wird, basiert auf einer proprietären Superpeer-Architektur [Baset & Schulzrinne 2006].

Napster und Gnutella sind bezeichnend für P2P-Systeme der ersten Generati-

[9] auch als Ultrapeers oder Supernodes bezeichnet

on. Sie wiesen zwar teilweise noch erhebliche Defizite auf, wie zum Beispiel hinsichtlich der eingeschränkten Skalierbarkeit, dennoch führte der immense Erfolg dieser Systeme – Napster wurde von ca. 65 Millionen Nutzern innerhalb der ersten 20 Monaten genutzt [Leuf 2002, S. 191] – zu einem *"P2P-Boom"*, welcher sich auch in Form von zahlreichen P2P-Systemen widerspiegelt, die seit dem Jahr 2000 entwickelt wurden.

2.2.2 P2P-Systeme und -Netze im Fokus der Wissenschaft

Die Popularität von Systemen wie Napster oder Gnutella im Internet rückte P2P-Systeme vermehrt in den Fokus der Wissenschaft [Steinmetz & Wehrle 2005a, S. 15]. Dabei versuchte man zunächst den Erfolg von bestehenden P2P-Systemen zu ergründen, um neue Systeme dementsprechend gestalten zu können. Ferner wurden im Kontext des P2P-Erfolgs auch bestehende wissenschaftliche Arbeiten nachträglich dem P2P-Bereich zugeordnet. So begann bspw. die Entwicklung von Anonymisierungsdiensten bzw. zensurresistenten Dienste wie Publius [Waldman et al. 2000] oder Freenet [Clarke et al. 2001], bevor sich P2P zu einem populären Thema entwickelte. Auch die Entwicklung von Overlay-Netzen wie dem *Resilient Overlay Networks (RON)*[10] [WWW Ron] begann unabhängig, ist jedoch im Nachgang als eines der ersten P2P-Netze zu sehen. Ebenso sind Multicast-Protokolle auf Anwendungsschicht dem P2P-Bereich zuzuordnen (vgl. u.a. [Chu et al. 2001] oder [Jannotti et al. 2000]).

Wie bereits aus der Hintergrundbetrachtung im vorigen Abschnitt deutlich wurde, kann man sich dem Thema P2P aus verschiedenen Richtungen näheren. Das Thema wurde daher in mehreren Disziplinen aufgegriffen [Crowcroft & Pratt 2002, S. 2]. Aufgrund des Netzwerkaspekts finden sich einerseits viele Arbeiten aus dem Bereich der Rechnernetze. Die Systemsicht spiegelt sich andererseits in den Arbeiten zu verteilten Systemen und Datenhaltung wider. Darüber hinaus entstand auch ein reges Interesse der Wirtschaftswissenschaften, da sowohl die Nutzung von Ressourcen als auch die Bereitstellung von Inhalten sich sichtlich von klassischen Systemen unterscheidet und somit das Potential für neuartige ökonomische Modelle eröffnet [Schoder & Fischbach 2003; Conrad et al. 2005a; Hummel et al. 2005].

Zu den ersten übergreifenden wissenschaftlichen Arbeiten im P2P-Bereich zählen insbesondere das Buch von A. Oram [Oram 2001] und die Arbeit von J. Crowcroft [Crowcroft & Pratt 2002] aus den Jahren 2001 und 2002. In den folgenden Jahren nahm die Anzahl der Veröffentlichungen explosionsartig zu, wie in Abschnitt 3.1.2 noch näher ausgeführt wird.

[10] Ziel des Projektes RON ist es, die Robustheit und Verfügbarkeit von Internet-Pfaden zu erhöhen, indem auf Anwendungsebene ein zusätzliches Routing durchgeführt wird.

Aus wissenschaftlicher Sicht widmete man sich zunächst vor allem der Frage, wie Daten, Dienste oder Ressourcen effizient gefunden werden können (vgl. u.a. [Stoica et al. 2001]). Eine wesentliche Entwicklung, die daraus hervorging, sind die so genannten *Verteilten Hash-Tabellen (engl. Distributed Hash Tables, DHT)*. Wie bei einer Hash-Tabelle üblich, können in einer DHT Schlüssel/Wert-Paare gespeichert werden, wobei die Schlüssel/Wert-Paare unter den Peers aufgeteilt werden, so dass es zu einer Verteilung der Last kommt. Die Knoten einer DHT erhalten hierfür eine eindeutige Kennung, anhand derer die Zuweisung der Schlüssel erfolgt. Durch die Knoten wird sodann ein Overlay-Netz aufgespannt, welches mittels der DHT-spezifischen Kennungen strukturiert wird. Eine vertiefte Einführung in solche P2P-Systeme und deren Eigenschaften erfolgt in Abschnitt 2.4.3.

Eine gewichtige Rolle aus wissenschaftlicher Hinsicht spielt das Projekt IRIS [WWW Iris], an dem unter anderem das MIT und die UC Berkeley beteiligt waren. Aus diesem Projekt gingen zahlreiche anerkannte Arbeiten und Systeme wie zum Beispiel die DHTs Chord, Pastry oder auch OpenDHT hervor, die im Folgenden noch Erwähnung finden.

2.3 Taxonomie

Aus der historischen Einführung in den vorigen Abschnitten und der Darlegung von bekannten Definitionen wird im Folgenden eine Definition für P2P-Systeme abgeleitet. Dabei ist zu beachten, dass die Definitionen nicht mit dem Ziel einer randscharfen Abgrenzung gestaltet wurden, vielmehr sollen insbesondere die charakteristischen Eigenschaften verdeutlicht werden. Ziel dieses Abschnitts ist es, grundlegende Begriffe zu definieren und in Bezug zueinander zu setzen. Außerdem wird eine explizite Abgrenzung zu den Bereichen Ad-hoc-Netzwerke und Grid vorgenommen.

2.3.1 Definition von P2P-Systemen

Vielfach wird der Begriff Peer-to-Peer bzw. P2P-System mittels einer Negativabgrenzung zum Client/Server-Paradigma (auf Rechnerebene[11]) definiert. In diesem Sinne beschreibt M. Singh das P2P-Paradigma in [Singh 2001] wie folgt: "P2P can be defined most easily in terms of what it is not: the client-server model."

Eine der ersten konkretisierten Definitionen des Begriffs P2P bzw. von P2P-Systemen, die auf große Akzeptanz gestoßen ist, wurde in dem Buch [Oram 2001]

[11] Im Folgenden bezieht sich, wenn nicht anders kenntlich gemacht, die Bezeichnung Server auf einen Rechner der ausschließlich als Dienstgeber auftritt und eine zentrale Position einnimmt.

von C. Shirky formuliert:

> *"Peer-to-peer is a class of applications that takes advantages of resources — storage, cycles, content, human presence — available at the edges of the Internet. Because accessing these decentralized resources means operating in an environment of unstable connectivity and unpredictable IP addresses, peer-to-peer nodes must operate outside DNS and have significant or total autonomy from central servers."*
> gemäß [Shirky 2001, S. 22].

Aus dieser Definition geht insbesondere hervor, dass es sich bei P2P-Systemen um eine Applikationsklasse handelt, deren Ziel es ist, Ressourcen, die sich am "Rande des Internet" befinden, nutzbar zu machen. Dies soll in einer dezentralen Weise ohne den Einsatz von zentralen Servern, erfolgen, wobei instabile Verbindungen und wechselnde IP-Adressen bei den Knoten berücksichtigt werden sollten.

Die vorgenannte Definition wurde unter anderem von R. Steinmetz und K. Wehrle aufgegriffen und in [Steinmetz & Wehrle 2004] bzw. [Steinmetz & Wehrle 2005a, S. 10] zu folgender Definition weiterentwickelt:

> *"[Ein P2P-System ist ein] sich selbst organisierendes System gleichberechtigter, autonomer Einheiten (Peers) […], das vorzugsweise ohne Nutzung zentraler Dienste auf der Basis eines Rechnernetzes mit dem Ziel der gegenseitigen Nutzung von Ressourcen operiert -- kurzum ein System mit vollständig dezentraler Selbstorganisation und Ressourcennutzung."*
> gemäß [Steinmetz & Wehrle 2004].

Bei dieser Definition ist insbesondere herausgehoben, dass die Knoten gleichberechtigt und autonom sind und das System als Ganzes möglichst dezentral[12] und selbstorganisierend gestaltet sein sollte. Zudem weist die Formulierung "auf der Basis eines Rechnernetzes" darauf hin, dass ein Overlay-Netz etabliert wird.

Eine weitere Definition wurde von S. Androutsellis-Theotokis und D. Spinellis in [Androutsellis-Theotokis & Spinellis 2004, S. 337] formuliert:

> *"Peer-to-peer systems are distributed systems consisting of interconnected nodes able to selforganize into network topologies with the purpose of sharing resources such as content, CPU cycles, storage and bandwidth, capable of adapting to failures and accommodating transient*

[12] In Bezug auf den Grad der Dezentralität bleibt die Definition etwas unklar, da in der schließenden Zusammenfassung von "vollständig dezentraler Selbstorganisation und Ressourcennutzung" die Rede ist, während zuvor die Formulierung "vorzugsweise ohne Nutzung zentraler Dienste" gebraucht wurde.

> *populations of nodes while maintaining acceptable connectivity and performance, without requiring the intermediation or support of a global centralized server or authority.*"
> gemäß [Androutsellis-Theotokis & Spinellis 2004].

Im Unterschied zu den vorigen Definitionen wird durch diese zum einen explizit gemacht, dass es bei P2P-Systemen um ein verteiltes System handelt. Zum anderen wird der Aspekt betont, dass sich die Menge der verfügbaren Knoten ständig ändert und das P2P-System somit adaptiv auf die Änderungen und Fehler reagieren muss, ohne dass die Aktivitäten zentral koordiniert werden.

Daneben existieren noch weitere Definitionen, die jedoch keine weiteren maßgeblichen Kriterien enthalten, so dass auf eine Vorstellung an dieser Stelle verzichtet werden kann.

Charakteristische Eigenschaften von P2P-Systemen: In den Arbeiten [Crowcroft & Pratt 2002], [Roussopoulos et al. 2005], [Kubiatowicz 2003] und [RFC 4981] wird keine explizite Definition von P2P-Systemen vorgenommen. Vielmehr wird das Themengebiet mittels charakteristischer Eigenschaften eingegrenzt. Bevor eine Definition des Begriffs P2P-System für diese Arbeit vorgenommen wird, erfolgt daher eine zusammengefasste Darstellung von Gesichtspunkten in Hinblick auf Ziele, Systemaufbau und kennzeichnende Eigenschaften, die in den genannten Arbeiten mit P2P-Systemen assoziiert werden:

- *Gemeinsame Ressourcennutzung* – Ziel eines P2P-Systems ist es, Ressourcen der beteiligten Knoten gemeinsam zu nutzen (engl. Resource Sharing). Die gemeinsame Ressourcennutzung kann dabei neben Systemressourcen wie CPU-Zyklen, Speicherplatz oder Bandbreite auch auf Ebene der Inhalte erfolgen.

- *Suche nach Ressourcen* – Ein zentrales Element von P2P-Systemen bildet die Suchfunktion, mittels derer die Lokation von Ressourcen identifiziert werden kann. Ohne diese Funktionalität wäre eine gemeinsame Ressourcennutzung nicht möglich und sie sollte daher, vor allem bei P2P-Systemen mit vielen Knoten, möglichst effizient hinsichtlich der notwendigen Anzahl von Nachrichten sein.

- *Massiv verteiltes System* – Ein verteiltes System ist ein System, bei welchem mehrere Komponenten, die sich auf vernetzten Rechnern befinden, an der Berechnung einer zugeteilten Aufgabe beteiligt sind [IEEE 1991]. Die Kommunikation und Koordination der Aktionen erfolgt dabei ausschließlich durch den Austausch von Nachrichten [Coulouris et al. 2005]. Ein P2P-

System besteht aus Knoten, die über Nachrichten kommunizieren und gemeinsam eine Aufgabe lösen. Da es in der Regel zahlreiche Knoten sind, handelt es sich insofern um ein massiv verteiltes System.

- *Overlay-Netze* – P2P-Systeme operieren auf Basis von Rechnernetzen, welche die Möglichkeit zur Kommunikation zwischen den Knoten bereits eröffnen. Durch ein P2P-System wird ein logisches Netz auf Anwendungsschicht etabliert, das als Overlay-Netz bezeichnet wird und im Allgemeinen in seiner Topologie unabhängig vom unterliegenden Rechnernetz ist.
- *Selbst-Organisation* – Zur Koordination der Knoten verwenden P2P-Systeme meist selbstorganisierende Mechanismen, so dass eine Funktion des Systems ohne manuelle Konfiguration ermöglicht wird (vgl. zur Selbstorganisation u.a. [de Meer & Koppen 2005]).
- *Dezentralität/Zentralität* – Trotz der Autonomie der Knoten ist ein P2P-System nicht zwangsläufig vollständig dezentral. So kommen teilweise zentrale Dienste, wie zum Beispiel zur Vergabe von Knotenkennungen zum Einsatz (vgl. bspw. Skype in Abschnitt 2.4).
- *Adaptivität* – Zum einen entscheiden Peers selbstständig über ihr Mitwirken und somit insbesondere auch über den Bei- und Austritt. Zum anderen handelt es sich häufig um "typische PCs", die sich ins Internet einwählen und nicht speziell robust ausgelegt sind. Insofern muss ein P2P-System adaptiv auf ständige Wechsel in der Menge der teilnehmenden Knoten reagieren, gleichgültig ob der Wechsel aus einem Systemfehler resultiert oder vom Nutzer initiiert war.
- *Symmetrische Rollenverteilung* – Im Gegensatz zu Client/Server-Systemen ist die Rollenverteilung zwischen den einzelnen Peers symmetrisch, so dass ein Knoten zu einem Zeitpunkt als Dienstgeber und zu einem anderen Zeitpunkt als Dienstnehmer auftreten kann (Client/Server-Paradigma auf Ebene der Software-Prozesse).
- *Autonomie der Peers* – Die einzelnen Peers unterstehen im Allgemeinen weder technisch noch organisatorisch einer zentralen Kontrolle. Daher können die Knoten autonom über den Zeitpunkt und Art der Mitwirkung am P2P-System entscheiden.
- *Autonomie des P2P-Systems* – Wenn das P2P-System über keine zentralen Entitäten verfügt und entsprechende selbstorganisierende Mechanismen integriert sind, kann das System als Ganzes auch autonom agieren, da für die Funktion des Systems keine Eingriffe von außen nötig sind.

Definition eines P2P-Systems: Abgeleitet aus den obigen Definitionen und den dargelegten charakteristischen P2P-Merkmalen ergibt sich die folgende Definition für P2P-Systeme, die dieser Arbeit zugrunde liegt:

> *Ein P2P-System ist ein massiv verteiltes System auf Basis eines Rechnernetzes, das sich aus einer Menge autonomer Peers zusammensetzt und vorzugsweise ohne Nutzung zentraler Dienste mit dem Ziel der gegenseitigen Nutzung von Ressourcen operiert, wobei zur Koordination der Peers vorwiegend selbstorganisierende Mechanismen eingesetzt werden. Ein P2P-System kann dabei adaptiv auf Peer-Wechsel (engl. Churn) sowie die Fehlfunktion einzelner Peers reagieren, und die Rollenverteilung zwischen den Peers ist symmetrisch.*

2.3.2 P2P-Ebenenmodell

Im vorigen Abschnitt wurde der Begriff *P2P-System* definiert, wie er in dieser Arbeit Verwendung findet. Daneben werden in der Literatur auch häufig die Begriffe *P2P-Netzwerk* und *P2P-Anwendung* gebraucht. Daher erfolgt in diesem Abschnitt eine Einordnung dieser Begriffe. Hierzu wird das Dreiebenenmodell [Schoder & Fischbach 2003] von D. Schoder und K. Fischbach aufgegriffen und weiterentwickelt.

Das ursprüngliche Modell besteht aus den drei Ebenen "P2P-Infrastrukturen", "P2P-Anwendungen" und "P2P-Gemeinschaften". Aufbauend auf einem Telekommunikationsnetzwerk folgt die erste Ebene, die als "P2P-Infrastrukturen" bezeichnet wird. In dieser ersten Ebene werden grundlegende Kommunikation- und Integrationsmechanismen bereitgestellt. Darauf aufbauend folgt die zweite Ebene der "P2P-Anwendungen", in welcher die anwendungsspezifischen Aspekte wie bspw. die Möglichkeit zum Dateitausch realisiert sind. Über diesen beiden technischen Ebenen folgt abschließend eine sozioökonomische Ebene, die als "P2P-Gemeinschaft" bezeichnet wird. Darunter wird eine Gemeinschaft von Personen verstanden, die ein gemeinsames Interesse wie bspw. das Interesse an Musik haben und im Rahmen einer solchen Gemeinschaft interagieren (vgl. auch [Parameswaran et al. 2001]). Die Kombination aller drei Ebenen wird von Schoder und Fischbach als "P2P-Netzwerk" bezeichnet. Dabei ist zu beachten, dass der Begriff P2P-Netzwerk, wie im Folgenden erläutert wird, im Rahmen dieser Arbeit anders verwendet wird.

Das Dreiebenenmodell wurde weiterentwickelt. Von dem ursprünglichen Modell abweichend, werden die drei Ebenen nicht als P2P-Netzwerk bezeichnet. Es werden vielmehr die beiden technischen Ebenen gemeinsam als P2P-System aufgefasst. Abb. 2.2 zeigt dieses weiterentwickelte Ebenenmodell.

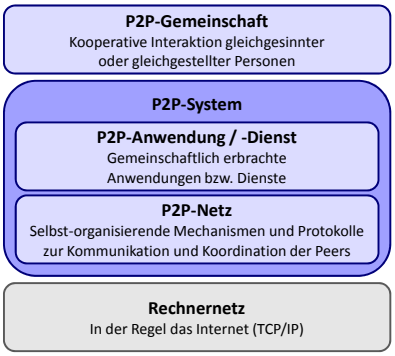


Abbildung 2.2: Dreiebenenmodell zur Differenzierung der Begriffe: P2P-System, -Netz, -Anwendung und -Gemeinschaft (abgeleitet von [Schoder & Fischbach 2003])

Die selbstorganisierenden Mechanismen und Protokolle zur Kommunikation und Koordination der Peers bilden als *P2P-Netz* die Grundlage für die Realisierung der darüberliegenden Anwendungen bzw. Dienste. Durch diese Mechanismen wird insbesondere die Struktur des Overlay-Netzes bestimmt. Gegebenenfalls werden hierzu P2P-spezifische Kennungen bzw. Adressierungsmechanismen sowie Routing-Verfahren festgelegt. Ferner werden die grundlegenden Mechanismen für die Verwaltung und Suche nach Ressourcen spezifiziert.

Auf der Ebene der *P2P-Anwendungen und -Dienste* werden applikationsspezifische Funktionen, wie zum Beispiel die Möglichkeit zum Dateitausch realisiert. Die Funktionen dieser Ebene nutzen wiederum die vom P2P-Netz bereitgestellten Funktionen. Wie im Abschnitt 2.4.4 anhand konkreter Systeme verdeutlicht wird, bedeutet dies jedoch nicht, dass eine P2P-Anwendung nur mittels des P2P-Netzes auf das unterliegende Kommunikationsnetz zugreifen kann. Wurde bspw. ein passendes Peer ermittelt, kann im Folgenden eine direkte Kommunikation auf IP-Ebene stattfinden. Die beiden technischen Ebenen P2P-Netz und P2P-Anwendungen/-Dienste bilden zusammen das *P2P-System*.

P2P-Gemeinschaften werden im Sinne von Schoder und Fischbach verstanden, d.h. sie bestehen aus einer Gruppe gleichgesinnter Personen[13], welche ein gemeinsames Ziel verfolgen bzw. gemeinsames Interesse teilen. P2P-Gemeinschaften bedingen nicht zwangsläufig ein P2P-System. So bilden viele Gruppen aus dem so genannten *Web 2.0*, wie zum Beispiel die Wikipedia-Teilnehmer eine P2P-Gemeinschaft. Die Systeme sind dabei technisch oft als Client/Server-Systeme realisiert. Ein weiteres Beispiel für eine P2P-Gemeinschaft stellt die Datenbank CDDB dar, durch welche die Titel von CDs und deren Lieder anhand der CD- bzw. Lied-Länge zugeordnet werden können und die Katalogisierung durch die

[13] auch als Teilnehmer bezeichnet

Nutzer selbst erfolgt [Oram 2001, S. 60]. Auch ein (elektronischer) Marktplatz, über welchen Produkte direkt zwischen den Teilnehmern gehandelt werden ist eine P2P-Gemeinschaft (vgl. auch Abschnitt 4.1.1).

Einige P2P-Systeme – vor allem die Systeme der ersten Generation – sind als monolithische Anwendungen realisiert, so dass die beiden technischen Ebenen nicht immer offensichtlich trennbar sind. Die Separierungsmerkmale werden anhand von ausgewählten P2P-Netzen und -Systemen in Abschnitt 2.4 verdeutlicht.

2.3.3 Abgrenzung von Ad-hoc-Netzen und Grid

Um dem Herkommen von P2P-Systemen sowie der breiten Basis existierender Systeme gerecht zu werden, lässt die vorgenannte Definition einen gewissen Interpretationsspielraum, so dass eine randscharfe Abgrenzung zu anderen Themengebieten nicht immer augenfällig ist. In den folgenden beiden Unterabschnitten wird eine Abgrenzung von P2P-Systemen zu Ad-hoc-Netzen und Grids vorgenommen, da diese beiden Themengebiete P2P-Systemen sehr nahe stehen und auch oft mit diesen in Zusammenhang gebracht werden.

Ad-hoc-Netzen

Drahtlose Kommunikation kann auf verschiedene Weisen organisiert werden. So können bspw. drahtlose lokale Netze (engl. Wireless LAN, WLAN) gemäß IEEE 802.11 sowohl im Infrastruktur- als auch im Ad-hoc-Modus betrieben werden. Beim Infrastruktur-Modus koordiniert die Basisstation die Kommunikation und alle Datenpakete werden über diese versendet. Eine direkte Kommunikation zwischen den Endgeräten findet dabei nicht statt. Die Basisstation nimmt daher eine herausgehobene, zentrale Stellung ein, vergleichbar einem Server bei Client/Server-Architekturen. Im Ad-hoc-Modus findet die Kommunikation ohne Basisstation direkt zwischen den Endgeräten statt und weist insofern Ähnlichkeiten zu Peer-to-Peer-Netzen auf, da die einzelnen Geräte autonom agieren und der Zugriff auf das geteilte Medium selbstorganisierend stattfinden muss. Teilweise wird in diesem Zusammenhang daher auch von Peer-to-Peer-Kommunikation gesprochen [Naraghi-Pour et al. 1998]. Die Ad-hoc-Kommunikation kommt insbesondere auch bei mobilen Netzen (engl. Mobile Ad-hoc Network, MANET) zum Einsatz und ist nicht auf IEEE 802.11 beschränkt.

Trotz der Ähnlichkeit in einzelnen Aspekten handelt es sich bei Ad-hoc-Netzen nicht um P2P-Netze. Das wesentliche Unterscheidungsmerkmal besteht darin, dass es sich bei P2P-Netzen im Unterschied zu Ad-hoc-Netzen um Overlay-Netze handelt, in welchen das unterliegende Netz bereits eine Kommunikation zwischen den Teilnehmern ermöglicht. Im Gegensatz dazu wird durch ein Ad-

hoc-Netz erst die Möglichkeit eröffnet zu kommunizieren. Ferner sind Ad-hoc-Netze in der Regel funkbasiert und daher in ihrer geographischen Ausdehnung begrenzt, während P2P-Netze oftmals globale Ausbreitung erlangen.

Grid-Computing

Die Begriffe *Grid* bzw. *Grid-Computing* wurden Mitte der 1990er Jahre durch geplante verteilte Rechnerinfrastrukturen geprägt, welche zur Unterstützung von rechen- bzw. speicherintensiven Aufgaben in der Spitzenforschung und Entwicklungen dienen sollten [Foster et al. 2001]. Durch die Assoziation mit dem englischen Ausdruck "Power Grid", zu deutsch Stromnetz, soll zum Ausdruck gebracht werden, dass der Zugriff auf die verteilten Rechnerressourcen ebenso einfach wie auf das Stromnetz erfolgen kann.

Eine erste Begriffsdefinition wurde von I. Foster und C. Kesselman in [Foster & Kesselman 1999] formuliert:

> *"A computational grid is a hardware and software infrastructure that provides dependable, consistent, pervasive, and inexpensive access to high-end computational capabilities."*
> gemäß I. Foster und C. Kesselman in [Foster & Kesselman 1999]

Aus dem Herkommen des Begriffs und dieser Definition werden zwei Dinge deutlich: Zum einen stehen Hochleistungsressourcen im Vordergrund (in diesem Sinne auch [Foster et al. 2001]) und zum anderen soll der Zugang möglichst einfach sein. Um dem zweiten Punkt gerecht zu werden, wurde in der Folge die Standardisierung von offenen, universellen Protokollen und Schnittstellen als eines der wichtigsten Ziele definiert [Foster et al. 2001].

Eine 3-Punkteliste, formuliert von I. Foster, grenzt den Begriff Grid weiter ein [Foster 2002]:

- Bei einem Grid handelt es sich um koordinierte Ressourcen, die keiner zentralen Kontrolle unterstehen, sondern zu unterschiedlichen administrativen Domänen gehören.
- Ein Grid wird durch offene, universelle Protokolle und Schnittstellen realisiert, mittels derer unter anderem eine Authentifizierung und Autorisierung stattfinden kann sowie eine Suche und ein Zugang zu den Ressourcen ermöglicht wird.
- Die Qualität der vom Grid erbrachten Dienste ist nicht "trivial", d.h. es können verschiedene Qualitätsstufen erbracht werden.

Aus Blickrichtung der gemeinsamen Ressourcennutzung geben sich die Gebiete Grid und P2P ähnlich. Beide ermöglichen es auf die Ressourcen anderer

zu zugreifen. Auch hinsichtlich des Gesichtspunkts unterschiedlicher administrativer Domänen verfolgt ein P2P-System durch die Autonomie der Peers ein gleichgelagertes Ziel. Bei näherer Betrachtung zeigen sich jedoch folgende Unterschiede:

- Im Allgemeinen integrieren Grids wesentlich leistungsfähigere Ressourcen als P2P-Systeme [Foster & Iamnitchi 2003, S. 120]. Bei Grid-Ressourcen handelt es sich in der Regel um dedizierte Ressourcen, während P2P-Systeme bereits vorhandene Ressourcen mitnutzen bzw. nutzbar machen.
- Der Fokus von Grids liegt darauf, die anfallende Last bzw. Aufgaben passend zu verteilen und im Fehlerfall Alternativen zu finden, wobei ein Fehler eine Ausnahme darstellt. Im Gegensatz dazu liegt von Hauptaugenmerk bei P2P-Systemen darauf, adaptiv auf wechselnde Teilnehmermengen und spontane Knotenausfälle zu reagieren [Androutsellis-Theotokis & Spinellis 2004, S. 338] – kurz gesagt: Fehler bilden bei Grids die Ausnahme, während sie bei P2P-Systemen der Normalzustand sind.
- Klassische Schutzziele der IT-Sicherheit wie Authentifizierung oder Autorisierung, aber auch das Abrechnungsmanagement sind bei Grids in der Regel unerlässlich [Foster & Iamnitchi 2003]. Bei P2P-Systemen handelt es sich hingegen meist um offene Systeme. Teilweise verschleiern die Systeme sogar die Identität der Nutzer (vgl. Anonymisierungsdienste in Abschnitt 2.4.4).

2.4 Ausgewählte P2P-Netze und -Systeme

Durch ausgewählte P2P-Netze und -Systeme soll in diesem Abschnitt ein "kennzeichnender Überblick" gegeben werden. Die Auswahl erfolgte dabei unter Berücksichtigung der wissenschaftlichen sowie der realweltlichen Relevanz. Eine vollständige Darstellung aller bekannten Netze und Systeme verbietet sich an dieser Stelle allein aufgrund der enormen Anzahl und wäre auch nicht zielführend, um die wesentlichen Aspekte zu verdeutlichen. Für eine umfassende Darstellung sei auf die überblicksartigen Arbeiten verwiesen, die in Abschnitt 2.5 vorgestellt werden.

Die Unterscheidung von P2P-Netzen folgt dabei der in der übrigen Literatur typischerweise vorgenommenen Klassifikation in hybride, unstrukturierte und strukturierte Netze[14] (vgl. u.a. [Aberer et al. 2003], [Androutsellis-Theotokis & Spinellis 2004], [Steinmetz & Wehrle 2004]):

[14] Unstrukturierte Netze definieren sich im Wesentlichen über die Negativabgrenzung zu strukturierten. Insofern werden in der folgenden Aufzählung zuerst die strukturierten erläutert.

- **Hybride P2P-Netze:** Ein P2P-Netz, das sowohl einen zentralisierten Dienst respektive Server als auch direkte P2P-Kommunikationsbeziehungen aufweist, wird als hybrides Netz bezeichnet.

- **Strukturierte P2P-Netze:** Die Topologie von strukturierten P2P-Netzen folgt einer Struktur, die durch P2P-spezifische Kennungen induziert wird. Kennzeichnend für strukturierte P2P-Netze ist auch, dass die Zuordnung von Ressourcen bzw. Verweise auf Ressourcen und Knoten mittels der P2P-spezifischen Kennungen stattfindet. Insofern können Suchanfragen innerhalb des P2P-Netzes gezielt weitergeleitet werden.

- **Unstrukturierte P2P-Netze:** Ein unstrukturiertes P2P-Netz setzt sich einzig aus Peers zusammen, wobei keine P2P-spezifischen Kennungen vorgesehen sind, anhand derer die Knoten strukturiert werden. Die Topologie ist daher vielmehr den Zufälligkeiten, wie zum Beispiel den Beitrittszeitpunkt und -ort unterworfen und insofern unstrukturiert. Die Peers haben in der Regel auch keine Information darüber, welches andere Peer welche Daten verwaltet bzw. über die von benachbarten Knoten bereitgestellten Ressourcen. Eine zielgerichtete Suche ist somit nicht möglich.

Die Anzahl der Knoten eines P2P-Netzes wird im Folgenden durch n angegeben. Eine Übersicht der verwendeten mathematischen Symbole findet sich im Anhang C.

2.4.1 Hybride Netze

Hybride Netze bestehen aus einer Menge von Peers und (mindestens) einer zentralen Komponente, die zur Koordination dient. Die Kernfunktion dieser zentralen Komponente besteht darin, eine Zuordnung von Ressourcen und Peers herzustellen. Insofern handelt es sich um ein zentrales Verzeichnis, das teilweise auch als Index bezeichnet wird. Um eine Ressource zu finden, sucht ein Peer mittels dieses zentralen Verzeichnis nach einem passenden Peer. Die folgende Ressourcennutzung findet dann zwischen den Peers direkt statt. In Abb. 2.3 ist solch eine hybrides Netz dargestellt. Napster oder die Tracker-basierte Variante von BitTorrent weisen eine solche Architektur auf (vgl. Abschnitt 2.4.4).

In der Abbildung wird mittels der Pfeile eine typische Ressourcennutzung veranschaulicht. Im ersten Schritt *(0)* veröffentlicht ein Peer die Ressourcen, welche es zur Verfügung stellt. Im folgenden Schritt *(1)* stellt ein anfragendes Peer eine Suchanfrage an das Verzeichnis, welches daraufhin die Adresse(n)[15] eines

[15]Unter der Adresse eines Peers wird eine Adresse des unterliegenden Netzes verstanden, so dass die Datenpakete dem entsprechenden Rechner und letztlich auch dem entsprechenden Soft-

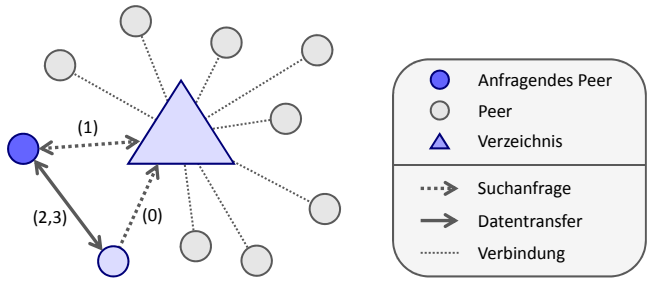


Abbildung 2.3: Hybrides P2P-Netz

oder mehrerer Peers übermittelt, welche die gesuchten Ressourcen bereitstellen. In den abschließenden Schritten *(2,3)* erfolgt die Ressourcennutzung. Wie in Abschnitt 2.3.1 ausgeführt, kann es sich bei den Ressourcen auch um Inhalte wie Dateien handeln.

Das Verzeichnis ist elementar für ein hybrides Netz, da ohne dieses keine Suche stattfinden kann und somit der nachfolgende Datentransfer nicht möglich ist. Werden Nutzerkennungen vergeben, wird hierzu in der Regel das Verzeichnis genutzt. Aus organisatorischer Sicht findet somit eine zentrale Steuerung statt.

Auch die Sprachtelefonie mittels eines SIP-Servers kann der Kategorie hybrides P2P-Netz zugeordnet werden, da die Verwaltung der SIP-Adressen mittels eines zentralen Verzeichnisses stattfindet und die folgende Kommunikation direkt zwischen den Teilnehmern erfolgen kann. Die Organisation mehrerer SIP-Server folgt einer Hierarchie, die durch das Domain Name System (DNS) induziert ist.

Aufgrund der zentralen Komponenten bezeichnen die Autoren in [Eberspächer & Schollmeier 2005] diese Architektur als zentralistisches P2P-System, während andere Autoren von einer hybriden Struktur sprechen [Steinmetz & Wehrle 2004]. Der Hauptgrund, weshalb solche Netze als P2P-Netze eingeordnet werden, ist historisch bedingt. Da Napster als erstes P2P-System gilt und eine solche Form aufweist, eröffnet man hierdurch die Möglichkeit Napster dem P2P-Bereich zuzuordnen. Obwohl Netze, die durch SIP-Server aufgespannt werden, gleicher Art sind, spricht man dort in der Regel von einer Client/Server-Architektur.

Die Skalierbarkeit ist durch das zentrale Verzeichnis begrenzt. Da aber nur die Suche und nicht die eigentlichen Ressourcen zentralisiert sind, sind solche Architekturen dennoch für viele Teilnehmer geeignet, wenn das Verzeichnis ausreichend dimensioniert ist. Nachteil solcher zentralen Ankerpunkte ist die Tatsache, dass sie *eine* einzelne kritische Fehlerstelle (engl. Single-Point-of-Failure) darstellen. Außerdem muss ein Betreiber für das zentrale Verzeichnis gefunden werden.

ware-Prozess zugestellt werden können. Im Falle des Internet also ein Tupel bestehend aus IP-Adresse sowie UDP- bzw. TCP-Port.

2.4.2 Unstrukturierte Netze

Im Gegensatz zu hybriden Netzen handelt es sich bei unstrukturierten und strukturierten P2P-Netzen um "reine" P2P-Netze [Eberspächer & Schollmeier 2005, S. 42], sie werden ausschließlich durch die teilnehmenden Peers gebildet.

Wie bereits zuvor ausgeführt, ist die gebildete Netztopologie bei unstrukturierten P2P-Netzen strukturlos. Sie ergibt sich durch zufällige Auswahl von Peers und ist abhängig vom Ort und Zeitpunkt des Netzbeitritt eines Peers. Unstrukturierte Netze können wiederum in die drei Kategorien *Fluten*, *Random Walk* und *Superpeer-Architekturen* unterteilt werden.

Fluten

Das bekannteste und zugleich erste P2P-Netz, welches auf dem Prinzip des Flutens basiert, ist Gnutella 0.4 [Ripeanu 2001]. Die Funktionsweise des Gnutella Protokolls ist denkbar einfach. In Abb. 2.4 ist der Ablauf einer exemplarische Suche verdeutlicht. Wenn ein Peer eine Ressource nutzen möchte, schickt es eine Suchanfrage an die benachbarten Knoten *(1)* und diese leiten die Suchanfrage wieder entsprechend weiter *(2)*. Dabei werden eingehende Nachrichten an alle bekannten Peers, außer dem Sender, weitergeleitet. Um die Ausbreitung zu begrenzen, werden Nachrichten, die bereits empfangen wurden oder deren "Lebenszeit" abgelaufen ist, nicht weitergeleitet. Hierzu enthält jedes Datenpaket eine eindeutige Kennung und einen so genannten Time-To-Live-Zähler (TTL-Zähler). In Abb. 2.4 wurde initial TTL $= 2$ angenommen. Wurde eine passende Ressource gefunden, wird eine Antwort auf dem gleichen Wege zurückgeschickt *(3,4)* und anschließend eine direkte Verbindung zwischen den Peers etabliert *(5,6)*.

Der TTL-Zählers begrenzt zwar die Suchanfragen (bei Gnutella gilt in der Regel TTL $= 7$ [Kan 2001, S. 106]), dennoch zeigt sich, dass das Protokoll bei typischem Nutzerverhalten nicht mit der Anzahl der Peers skaliert, da in Summe

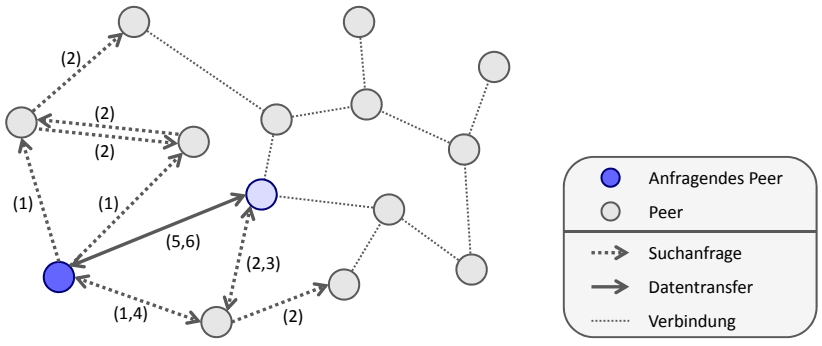


Abbildung 2.4: Verbreitung einer Suchanfrage bei Gnutella durch *fluten*

zu viele Nachrichten pro Suchanfrage entstehen und bei einem zu geringen TTL-Wert die Suchanfragen nicht mehr ausreichend viele Knoten erreichen [Lv et al. 2002]. Durch Beschränkung der Ausbreitung einer Suchanfrage kann es außerdem dazu kommen, dass eine Ressource nicht gefunden wird, obwohl ein Peer diese bereitstellt.

Da jedes Peer die Suchanfragen lokal auswertet, realisiert jedes Peer auch ein lokales Verzeichnis. Vorteilhaft dabei ist die Unabhängigkeit der Suchanfragen vom P2P-Netz. Somit können bspw. auch komplexe Suchanfragen mit Schlagwörtern, Meta-Daten oder Jokerzeichen (engl. Wildcards) realisiert werden.

Random Walk

Im Gegensatz zum Fluten wird eine Suchanfrage bei einem so genannten Random Walk immer nur an *einen* benachbarten Knoten weitergeleitet. Abb. 2.5 zeigt den Ablauf einer beispielhaften Suchanfrage mittels eines Random Walks. Bei Random Walks wird die TTL wesentlich größer gewählt als beim Fluten, da sich die Anzahl der Nachrichten nicht bei jedem Peer vervielfacht, sondern konstant bleibt und ansonsten keine ausreichende Verbreitung der Suchanfrage gewährleistet werden kann.

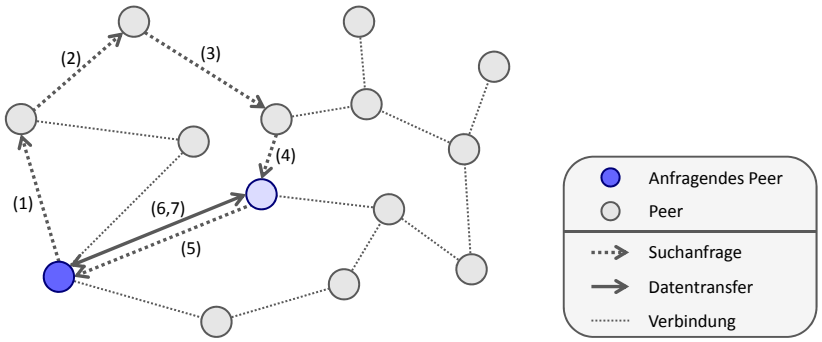


Abbildung 2.5: Verbreitung einer Suchanfrage mittels Random Walk

In [Lv et al. 2002] wird gezeigt, dass durch mehrere parallele Random Walks die Skalierbarkeit im Vergleich zum Fluten wesentlich gesteigert werden kann, da die Anzahl der notwendigen Nachrichten deutlich reduziert wird und dennoch eine gute Ausbreitung der Suche erreicht wird. Dabei wird insbesondere auch die Replikation von Inhalten gemäß [Cohen & Shenker 2002] berücksichtigt. Es bleibt jedoch zu beachten, dass eine Replikation nicht bei jeglichen Ressourcen durchführbar ist. Bei Systemressourcen kann bspw. keine Replikation erfolgen. Eine Alternative zur Replikation der Ressourcen selbst stellt die Replikation der lokalen Verzeichnisse dar. In dem unstrukturierten P2P-Netz GIA wird diese Technik erfolgreich mit Random Walks kombiniert [Chawathe et al. 2003].

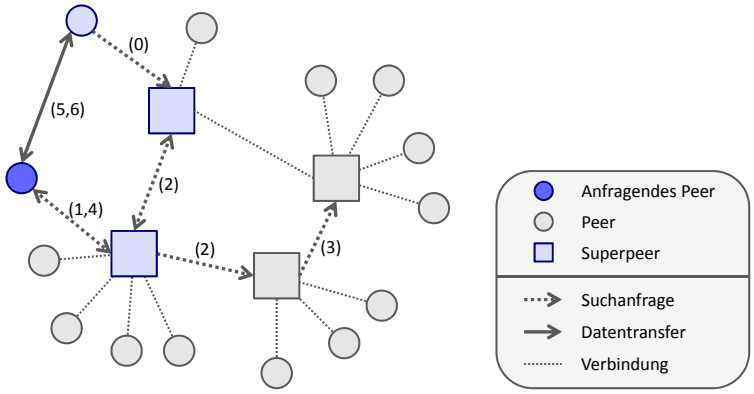


Abbildung 2.6: Unstrukturiertes P2P-Netz mit Superpeers

Superpeer-Architektur

Die ersten Vorschläge zu Superpeer-Architekturen entstanden im Zusammenhang mit der Weiterentwicklung des Gnutella-Protokolls. So wurde in [Singla & Rohrs 2002] vorgeschlagen, Knoten in Leafs und Ultrapeers zu unterteilen. Statt Ultrapeer wird mittlerweile häufiger die Bezeichnung Superpeer verwendet. Wie in Abb. 2.6 dargestellt, sind Leaf-Peers in der Regel nur mit einem Superpeer verbunden. Ein Leaf-Knoten teilt dem Superpeer im ersten Schritt *(0)* mit, welche Ressourcen es bereitstellt. Sucht nun ein anderes Peer Ressourcen, leitet es die Suchanfrage an das zugehörige Superpeer weiter *(1)*. Die Suchanfrage wird dann zwischen den Superpeers ausgetauscht *(2,3)*. Wird ein passendes Peer gefunden, wird die Adresse dem suchenden Peer mitgeteilt *(4)*[16]. Die folgende Ressourcennutzung findet wiederum direkt zwischen den Peers statt *(5,6)*. Für die Kommunikation zwischen den Superpeers kann dabei Gnutella oder auch ein anderes P2P-Protokoll Verwendung finden.

Die Auswahl der Superpeers erfolgt unter Berücksichtigung der Bandbreite und gegebenenfalls der Sitzungsdauer, d.h. der Zeit, wie lange ein Peer aktiv ist. Es werden Peers bevorzugt, die breitbandig angebunden und langlebig sind. Außerdem ist Anzahl der Superpeers wesentlich geringer als die Zahl der Leafs. Um den Superpeers eine Auswertung der Suchanfrage zu ermöglichen, teilen die Leafs dem Superpeer die angebotenen Ressourcen mit. Insofern wird von Superpeers eine Aggregation der lokalen Verzeichnisse der konnektierten Leafs vorgenommen. Durch die eingeführte Hierarchie und die spezielle Auswahl der Superpeers kann schließlich die durch Suchanfragen verursachte Anzahl an Nachrichten wesentlich reduziert werden.

Neben Gnutella basieren noch weitere P2P-Systeme, wie zum Beispiel Skype

[16]Bei Gnutella 0.6 wird die Suchanfrage von den Superpeers zu potentiellen Leafs weitergereicht, um sicherzustellen, dass der Leaf die gesuchte Ressource noch bereitstellt.

auf Superpeer-Architekturen (vgl. [Baset & Schulzrinne 2006]). Auch das proprietäre P2P-Protokoll Fasttrack, das von der Firma Sharman Networks entwickelt wurde und der Musiktauschbörse Kazaa zugrunde liegt, nutzt Superpeers [WWW Sharman].

2.4.3 Strukturierte Netze

Die Topologie von strukturierten Netzen ist durch Peer-spezifische Kennungen bestimmt und ermöglicht es Nachrichten gezielt weiterzuleiten im Gegensatz zu unstrukturierten Netzen, bei welchen die Nachrichten mehr oder weniger "blind" weitergeleitet werden. Insofern wird auch ein eigenes Adressierungsschema etabliert.

Im Wesentlichen werden strukturierte Netze als verteilte Hash-Tabellen (engl. Distributed Hash Table, DHT) realisiert. Wie bei Hash-Tabellen üblich, können darin Schlüssel/Wert-Paare gespeichert und abgefragt werden. Ziel von DHTs ist es, die Hash-Tabelle zwischen den aktiven Peers gleichmäßig aufzuteilen und ein effizientes Routing-Verfahren zu realisieren, um das zuständige Peer möglichst schnell und mittels weniger Nachrichten zu finden. Für ein effizientes Routing ist es dabei nicht zielführend, alle anderen Peers zu kennen, da zum einen die notwendige Routing-Tabelle sehr groß werden kann und zum anderen der Overhead, der beim Bei- und Austritt eines Peers entstünde, zu groß wäre.

Ausgangspunkt dieser Systeme bildet eine Arbeit von C. Plaxton et al. aus dem Jahr 1997 [Plaxton et al. 1997]. In der Arbeit wird ein randomisiertes Zugriffsschema entwickelt, dass es ermöglicht schnell auf im Netzwerk verteilte Objekte zu zugreifen, wobei der notwendige Overhead in Form von Verzeichnissen bzw. Verweisen möglichst gering gehalten wird. Die vereinfachten Grundzüge der Arbeit sind auch in Chord enthalten [Stoica et al. 2001, S. 150].

Im Folgenden werden exemplarisch das Chord- und das Kademlia-Protokoll erläutert. Das Chord-Protokoll wurde gewählt, da es ein typischer Vertreter für DHTs ist und sich die wesentlichen Sachverhalte anschaulich verdeutlichen lassen. Die Auswahl des Kademlia-Protokoll erfolgte vor allem aufgrund seiner Praxisrelevanz (vgl. Abschnitt 3.1).

Chord

Chord wurde als Nachschlagedienst (engl. Lookup Service) für Internet-Applikationen entwickelt [Stoica et al. 2001]. Der Dienst realisiert eine DHT und ermöglicht es somit, Schlüssel/Wert-Paare zu speichern und abzufragen. Den Peers wird jeweils eine eindeutige Kennung *ID* aus einem flachen Adressraum von 0 bis $2^z - 1$

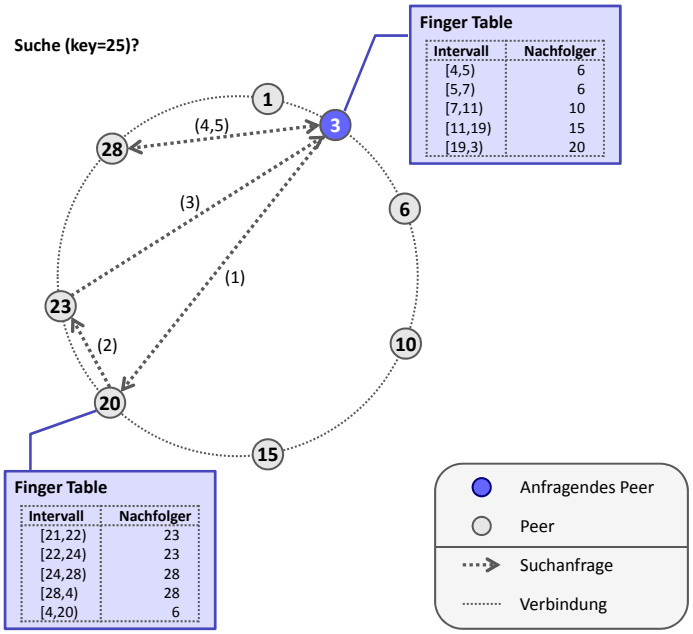


Abbildung 2.7: Rekursives Routing in einem Chord-Netz

zugeteilt (meist wird $z = 160$ gewählt)[17]. Im Internet kann die Kennung bspw. bestimmt werden, indem ein Hash über die IP-Adresse berechnet wird [Stoica et al. 2001]. Im Sinne einer kompakteren Darstellung wurde in Abb. 2.7 und 2.8 der Raum der Knotenkennungen auf $z = 5$ begrenzt. In den Abbildungen haben die Peers die *IDs* $1, 3, 6, \ldots, 28$ erhalten, wobei auf die *ID* $2^z - 1$ wieder die *ID* 0 folgt, so dass sich ein Ring ergibt.

Für die Schlüssel der Schlüssel/Wert-Paare wird ebenso wie für die Knotenkennungen ein Schlüsselraum festgelegt, welcher im Fall von Chord den gleichen Umfang wie der Raum der *IDs* hat. Durch eine Abbildung vom Schlüsselraum auf den Raum der Knotenkennungen wird bestimmt, welcher Knoten für einen bestimmten Schlüssel zuständig ist. Bei Chord ist der Knoten zuständig, dessen *ID* gleich dem Schlüssel ist oder als nächste folgt. In dem exemplarischen Chord-Netz in der Abb 2.7 ist Knoten *28* daher für die Schlüssel 24 bis 28 zuständig. Um eine gleichmäßige Verteilung der Schlüssel zu erreichen, sollte die P2P-Anwendung die Schlüssel mittels einer konsistenten Hash-Funktion (engl. Consistent Hashing) wie zum Beispiel SHA-1 [FIP 180-1] berechnen (vgl. zu konsistenten Hash-Funktionen [Karger et al. 1997]).

Soll nun ein Wert für den Schlüssel 25 gespeichert oder dessen Wert abgefragt werden, muss eine Kommunikation mit dem Knoten 28 erfolgen. Eine notwendi-

[17] In [Stoica et al. 2001] wird der Parameter z als m bezeichnet. Im weiteren Verlauf dieser Arbeit wird m jedoch als die Anzahl der Nachbarknoten eines Knotens definiert (vgl. auch Anhang C).

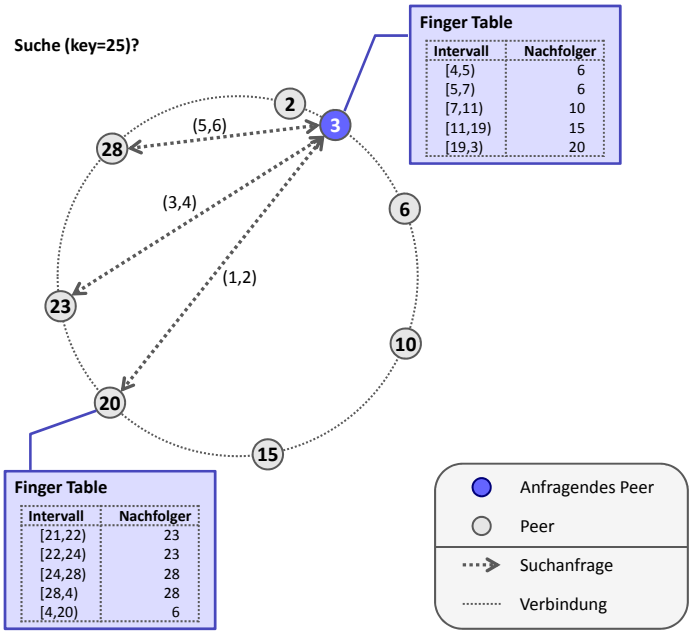


Abbildung 2.8: Iteratives Routing in einem Chord-Netz

ge und hinreichende Bedingung für das Chord-Netz ist, dass jeder Knoten seinen Nachfolger im Sinne der *IDs* kennt. Wenn dies die einzige Routing-Information der Knoten wäre, würde eine Suchanfrage jedoch so lange im Ring weitergeleitet werden bis der zuständige Knoten erreicht ist. Wie unschwer erkennbar ist, würde dies im Durchschnitt zu $O(n)$ Routing-Schritten führen, wobei n der Anzahl der aktiven Knoten entspricht. Daher pflegt jeder Knoten zusätzlich eine so genannte Finger Table, in welcher weitere Knoten verzeichnet sind. Für Knoten i werden die k Einträge $(\mathtt{finger}_{i,k}, \mathtt{Knotenadresse})$ der Finger Table wie folgt berechnet: Zunächst werden die *IDs* berechnet mit $\mathtt{finger}_{i,k} = (i + 2^{k-1}) \bmod 2^z$, $1 \leqslant k \leqslant z$, wobei i der *ID* des Knotens entspricht. Das Intervall ergibt sich dann zu $[\mathtt{finger}_{i,k}, \mathtt{finger}_{i,k+1} - 1)$. In der Finger Table wird dann jedem $\mathtt{finger}_{i,k}$ der nachfolgende Knoten und dessen Adresse zugeordnet. Durch die zusätzlichen Routing-Informationen der Finger Table kann letztlich eine Weiterleitung der Nachricht zum zuständigen Knoten in $O(\log n)$ Schritten erfolgen.

Abb. 2.7 zeigt exemplarisch die Weiterleitung der Suchanfrage mit dem Schlüssel 25 von Knoten 3 ausgehend. Da jeder Knoten seinen unmittelbaren Nachfolger kennt, aber nicht zwangsläufig seinen Vorgänger, wird zunächst der Knoten ermittelt dessen Nachfolger zuständig ist, also Knoten *23*. Anschließend erfolgt eine direkte Kommunikation mit dem zuständigen Knoten *28*. Die Finger Tables bei Chord sind asymmetrisch und eine Weiterleitung der Nachrichten erfolgt im Ring nur in aufsteigender Richtung.

Für eine detaillierte Beschreibung der Funktionsweise sei auf [Stoica et al.

2001] verwiesen, worin insbesondere auch erläutert wird, wie sich neue Knoten in das Netz integrieren und Knotenausfälle kompensiert werden. In der Arbeit wird auch ein Nachweis geführt, dass (mit hoher Wahrscheinlichkeit[18]) nur $O(\log n)$ Schritte notwendig sind, um den zuständigen Knoten zu erreichen und das bei der Integration eines neuen Knotens auch nur $O(\log n)$ Finger Tables angepasst werden müssen.

Im Gegensatz zum Beispiel in Abb. 2.7, in welchem eine *rekursive* Weiterleitung der Suchanfrage erfolgte, kann die Weiterleitung auch *iterativ* erfolgen, wie dies in Abb. 2.8 veranschaulicht ist. Bei der iterativen Weiterleitung ist die summierte Latenzzeit zwar höher, aber der suchende Knoten kann wesentlich schneller erkennen wenn eine Nachricht verloren geht oder ein Knoten sich nicht protokollkonform verhält (vgl. insofern auch die Weiterleitung von DNS-Anfragen).

Soll ein DHT-basiertes System zum Dateitausch realisiert werden, könnte man einen Hash über die Datei berechnen und die Datei beim zuständigen Knoten speichern. In der Regel wird man jedoch vielmehr eine weitere Indirektionsstufe einfügen und nicht die Datei selbst als Wert speichern, sondern nur einen Verweis auf den Knoten, welcher die Datei tatsächlich vorhält. Insofern realisiert eine DHT dann ein verteiltes Verzeichnis. Im Rahmen des so genannten Trackerless-Modus von BitTorrent (vgl. folgender Abschnitt) wird solch ein Verfahren erläutert.

Kademlia

Das P2P-Netz Kademlia [Maymounkov & Mazieres 2002] ermöglicht es, wie bei DHT-basierten P2P-Netzen üblich, Schlüssel/Wert-Paare zu speichern. Kademlia liegt ein eindimensionaler *ID*-Raum $\{0 \dots 2^z - 1\}$ zugrunde, wobei in der Regel $z = 160$ gewählt wird. Die Schlüssel der Schlüssel/Wert-Paare stammen dabei aus dem gleichen Raum.

Die Knoten in Kademlia werden als Blätter in einem Binärbaum aufgefasst, wie in der Abb. 2.9 exemplarisch dargestellt. Die Knoten haben bei dieser Abbildung die Kennungen $2, 3, 6, \dots, 28$ und der Adressraum wurde auf $z = 5$ beschränkt. Die Position der Knoten im Binärbaum bestimmt sich dabei durch den kürzesten eindeutigen Präfix der binär interpretierten Knotenkennung.

Ferner zeigt Abb. 2.9 durch die gestrichelten Rahmen so genannte Subbäume ausgehend von dem Knoten 3. Diese Subbäume sind Teilbäume, in welchen der Knoten 3 nicht enthalten ist und ergeben sich indem der Präfix des Knotens verkürzt wird, wie in den Routing-Tabellen in Abb. 2.9 dargestellt. Das Kademlia-

[18] Nach [Karger et al. 1997, S. 656] meint der Ausdruck "mit hoher Wahrscheinlichkeit" eine Wahrscheinlichkeit von mindestens $1 - 1/Q$, wobei Q ein Konfidenzparameter darstellt (vgl. auch die Diskussion in [Stoica et al. 2001, S. 152]).

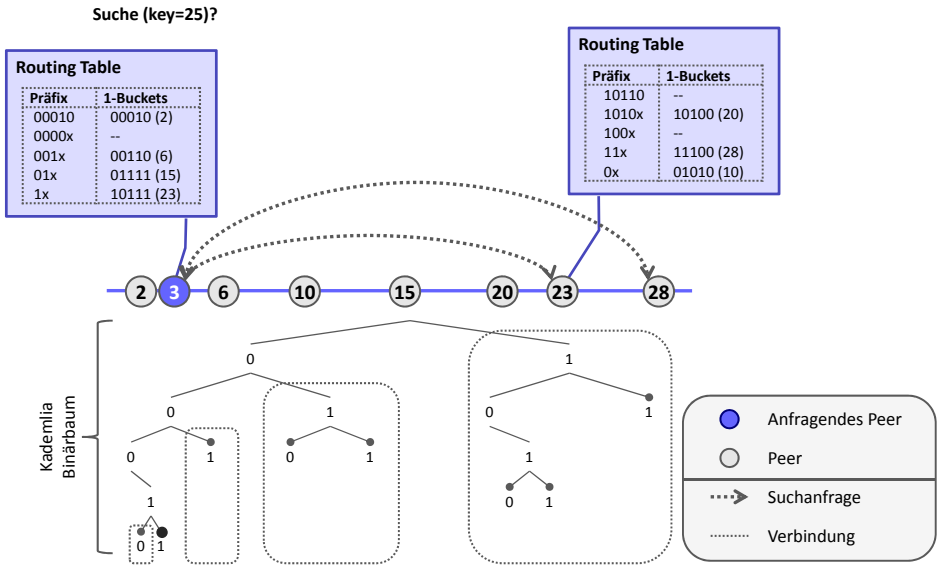


Abbildung 2.9: Exemplarische Suche in einem Kademlia-Netz

Protokoll garantiert, dass jeder Knoten mindestens einen Knoten in jedem Subbaum kennt, wenn der Subbaum einen Knoten enthält. Es kann auch garantiert werden, dass jeder Knoten nach endlich vielen Schritten gefunden wird.

Für die Abbildung von Schlüsseln auf Knoten und das Routing wird bei Kademlia eine so genannte XOR-Metrik genutzt. Diese ist folgendermaßen definiert: Der Abstand $d(x, y)$ zwischen zwei *IDs* x und y ergibt sich, indem x und y zunächst Bit-weise XOR-verknüpft werden und die resultierende Bitfolge als Integer-Zahl interpretiert wird.

Ein Knoten ist dann für einen Schlüssel zuständig, wenn der Abstand zwischen der Knotenkennung und dem Schlüssel minimal ist, d.h. es keinen Knoten gibt dessen *ID* einen geringen Abstand zu dem Schlüssel hat. Aus Gründen der Robustheit wird ein Schlüssel/Wert-Paar in der Regel nicht nur auf dem nächsten, sondern den k nächsten Knoten gespeichert.

Zum Weiterleiten von Nachrichten besitzt jeder Knoten eine Liste mit so genannten k-Buckets, wobei k der Anzahl der Einträge eines Buckets entspricht. In Abb. 2.9 ist $k = 1$. In realweltlichen Systemen wie der BitTorrent-DHT wird $k = 8$ verwendet. Für jedes der $0 \leqslant i < z$ k-Buckets gilt[19], dass die darin enthaltenen Nachbarknoten einen Abstand zwischen 2^i und 2^{i+1} zur *ID* des Knotens haben, was den Subbäumen in Abb. 2.9 entspricht.

Die Weiterleitung der Nachrichten erfolgt iterativ. Der anfragende Knoten ist

[19] Eine in [Maymounkov & Mazieres 2002] beschriebene Variante von Kademlia fasst mehrere Buckets zusammen. Dabei wird durch den Parameter b angegeben um wie viele Bits der Präfix sich jeweils unterscheidet. Bei der beschriebenen Version ist $b = 1$.

daher in jedem Kommunikationsschritt involviert. Abb. 2.9 zeigt eine Suchanfrage nach dem Schlüssel 25. Zunächst wird dabei der Knoten 23 kontaktiert, welcher wiederum auf Knoten 28 verweist.

In Kademlia stehen folgende vier Operationen zur Verfügung:

- `Find_Node`: Durch Angabe eines Schlüssel wird mittels dieser Operation, der zum angegebenen Schlüssel nächste Knoten bestimmt.
- `Find_Value`: Diese Operation verhält sich wie die `Find_Node`-Operation. Außer wenn ein Knoten ein zum angegebenen Schlüssel passendes Schlüssel/Wert-Paar speichert, wird der entsprechende Wert zurück gegeben.
- `Ping`: Mittels dieser Operation wird die Erreichbarkeit von Knoten überprüft.
- `Store`: Die `Store`-Operation dient dazu einen Schlüssel/Wert-Paar beim zuständigen Knoten zu speichern. Der zuständige Knoten wird dabei zuvor durch die `Find_Node`-Operation bestimmt.

Um die Buckets aktuell zu halten, werden in regelmäßigen Abständen, im Weiteren als Aktualisierungsintervall bezeichnet, passende Knoten mittels der `Find_Node`-Operation gesucht bzw. die Erreichbarkeit von bekannten Knoten durch `Ping`-Nachrichten überprüft. Darüber hinaus kann ein Knoten durch die Suchanfragen, welche an ihn gerichtet sind auch passiv lernen, da diese jeweils die Knotenkennung des anfragenden Knoten enthalten. Ist ein anfragender Knoten bereits in den Buckets enthalten, muss die Erreichbarkeit nicht gesondert überprüft werden.

Insgesamt kann gezeigt werden, dass das Routing bei Kademlia mit hoher Wahrscheinlichkeit $O(\log n)$ Hops benötigt. Im Gegensatz zu Chord, bei welchem die Knoten in einer strikten Struktur organisiert sind, sind die Invarianten bei Kademlia etwas gelockert. So können bei der Auswahl der Knoten weitere Faktoren wie die Lebenszeit von Knoten oder auch die Latenzzeiten einbezogen werden. Beim Routing werden insbesondere langlebige Knoten bevorzugt.

Weitere strukturierte P2P-Netze

Neben den beiden vorgestellten DHT-basierten P2P-Netzen wurde noch eine Reihe weiterer Systeme entwickelt (Die folgende Liste enthält nur eine Auswahl.):

- *Content Addressable Network (CAN):* Im Gegensatz zu Chord oder Kademlia basiert das P2P-Netz CAN auf einem mehrdimensionalen Raum, der in gleichmäßige Zonen aufgeteilt wird [Ratnasamy et al. 2001a]. Ein Peer ist dabei für jeweils eine Zone zuständig.

- *Pastry:* Ein wesentliches Merkmal von Pastry ist, dass die Latenzzeiten des unterliegenden Netzes explizit berücksichtigt werden [Rowstron & Druschel 2001].
- *Erweiterungen von Chord:* Erweiterungen von Chord finden sich unter anderem in Koorde [Kaashoek & Karger 2003], Symphony [Manku et al. 2003] und Viceroy [Malkhi et al. 2002].

Bei *P-Grid* [Aberer et al. 2002] handelt es sich im Wesentlichen auch um ein strukturiertes P2P-Netz, wobei probabilistische Algorithmen zum Einsatz kommen, so dass die Struktur etwas variieren kann, aber dennoch gezielt Suchanfragen weitergeleitet werden können. Darüber hinaus gibt es auch Netztopologien, welchen ein Hyperkubus zugrunde liegt (vgl. u.a. [Schlosser et al. 2002]).

2.4.4 P2P-Systeme

Neben Dateitauschsystemen können P2P-Systeme auch in weiteren Bereichen zum Einsatz kommen. Wesentliche Anwendungsbereiche werden im Folgenden kurz aufgezeigt:

- *Dateitauschsysteme:* Die ersten P2P-Systeme Napster und Gnutella waren bereits Dateitauschsysteme. In der Folge wurden zahlreiche Weitere entwickelt, wobei zu den bekanntesten BitTorrent und Kazaa zählen.

- *Kommunikationslösungen:* P2P-basierte Lösungen kommen auch als Kommunikationslösung für Sprachtelefonie und Instant Messaging zum Einsatz. Typische Vertreter dieser Kategorie sind Dienste wie Skype oder auch P2P-SIP, d.h. die Realisierung von SIP-basierter Kommunikation ohne SIP-Server [RFC 3261].

- *Verzeichnisdienste:* Durch das OpenDHT-System [WWW OpenDHT] wird ein öffentlich zugänglicher DHT-Dienst bereitgestellt, in welchem zu einem 20-Byte Schlüssel ein Wert von maximal 1024 Byte hinterlegt werden kann. In [Rhea et al. 2005b] wird dargestellt, wie sich OpenDHT für verschiedene Anwendungen nutzen lässt.

- *Video-Streaming:* Ferner eignen sich P2P-Systeme auch, um Videos oder TV-Übertragungen effizient zu verteilen. Bekannte Vertreter für diesen Bereich sind Joost [WWW Joost] und PPLive [Huang 2007]. Eine Übersicht solcher Systeme findet sich in [Liu et al. 2008].

- *Multicast und Anycast:* Zahlreiche P2P-Systeme wurden entworfen, um auf Applikationsebene (meist mittels einer DHT) eine Multicast- oder Anycast-

Kommunikation zu ermöglichen. Eines der ersten Systeme wird in [Ratnasamy et al. 2001b] beschrieben. Auch die im folgenden Abschnitt beschriebene Internet Indirection Infrastructure lässt eine Multicast- und Anycast-Kommunikation zu [Stoica et al. 2002].

– *Anonymisierungsdienste:* Die Entwicklung von Systemen zur zensurresistenten Veröffentlichung von Dokumenten bzw. zur anonymen Kommunikation fand weitgehend unabhängig und teilweise auch vor der Entwicklung der ersten P2P-Systeme statt (vgl. u.a. [Chaum 1981] zu nicht rückverfolgbaren E-Mails). Dennoch sind die Systeme teilweise als P2P-Systeme realisiert. Eines der ersten P2P-ähnlichen Systeme aus dem Jahr 1996, ist das Eternity-System [Anderson 1996]. Weitere Systeme wie Freenet [Clarke et al. 2001] und Tor [Dingledine et al. 2004] folgten.

Im Folgenden werden konkrete P2P-Systeme kurz eingeführt und anhand derselben das Funktionsspektrum verdeutlicht. Diese Systeme dienen im weiteren Verlauf der Arbeit auch zur Illustration einzelner Sachverhalte.

BitTorrent

Bei BitTorrent [WWW BitTorrent] handelt es sich um ein Dateitauschsystem, welches von B. Cohen entwickelt wurde und vor allem für die Verteilung großer Dateien mit mehreren 100 MByte konzipiert ist. So werden bspw. Linux-Distributionen über dieses System zur Verfügung gestellt. Da BitTorrent für große Dateien konzipiert ist, wird auch eine Aufteilung der Dateien, in so genannte Chunks, unterstützt. Teile einer Datei können somit von unterschiedlichen Peers bezogen werden. Um für Knoten einen Anreiz zu schaffen, bereits bezogene Chunks anderen zum Download anzubieten, wurde ein so genanntes Tit-for-Tat-Verfahren (zu deutsch: “wie du mir, so ich dir”-Verfahren) implementiert [Cohen 2003].

Die ursprüngliche BitTorrent-Architektur gleicht der von Napster insofern, dass es einer zentraler Komponente, den so genannten *Tracker*, bedarf, der die Koordination zwischen den Peers übernimmt. Daher handelt es sich bei der Tracker-basierten Variante von BitTorrent um ein hybrides Netz. Im Gegensatz zu Napster kann es jedoch pro Datei einen eigenen Tracker geben. Die Adresse des Trackers sowie Hashes über die Datei als Ganzes und die einzelnen Chunks sind in einer so genannten *torrent*-Datei, kurz *torrent*, zusammengefasst. BitTorrent bietet keine Unterstützung, um *torrents* zu suchen. Diese werden daher über andere Mechanismen wie Websites ausgetauscht.

Das wesentliche Augenmerk von BitTorrent liegt darauf, möglichst effizient Inhalte zwischen den interessierten Peers zu verteilen. In [Izal et al. 2004] wurde gezeigt, dass sich bei der Verteilung einer Linux-Distribution im Jahr 2004

durch solch ein System eine kumulierte Bandbreite bis zu 800 Mbit/s ergab, obwohl die Anbindung der einzelnen Knoten um ein Vielfaches geringer war. Auf eine gewisse Weise kann mittels BitTorrent somit auch Bandbreite auf Abruf (engl. Bandwidth on Demand) zur Verfügung gestellt werden.

Um die Abhängigkeit von zentralen Trackern zu reduzieren, wurde mittlerweile zusätzlich ein *Trackerless*-Modus in BitTorrent integriert. Dieser basiert auf dem P2P-Netz Kademlia[20]. Die Funktion des Trackers wird dabei von einem bzw. mehreren Knoten der DHT übernommen, wobei die DHT von allen BitTorrent-Knoten gemeinsam gebildet wird. Die zuständigen Knoten pflegen jeweils eine Liste der Peers, die eine Datei anbieten. Als Schlüssel dient der Hash über die entsprechende *torrent*-Datei und als Wert wird eine Liste von IP-Adressen nebst Ports von Peers gepflegt, welche die Datei oder Teile der Datei anbieten. Während eine DHT im Allgemeinen das Speichern von beliebigen (nur in der Größe beschränkten) Schlüssel/Wert-Paaren zulässt, speichert die BitTorrent-DHT zu einem gegebenen Schlüssel nur die IP-Adresse und den Port.

Die meisten Peers in BitTorrent haben insofern eine Doppelfunktion: Zum einen implementieren sie das BitTorrent-Protokoll gemäß [BitT BEP3 2008] zum Austausch von Dateien. Zum anderen enthalten aktuelle Implementierungen, wie zum Beispiel µTorrent einen DHT-Teil entsprechend [BitT BEP5 2008]. Da die DHT durch alle BitTorrent-Knoten gebildet wird, ist mit hoher Wahrscheinlichkeit ein Knoten für die Pflege der Peer-Liste zu einem *torrent* zuständig, der selbst an der Datei kein Interesse hat.

Skype

Bei Skype handelt es sich um eine P2P-Anwendung, mittels derer insbesondere Sprachtelefonie und Instant Messaging möglich ist. Skype wird durch eine proprietäre Anwendung, welche auch ein proprietäres P2P-Protokoll implementiert, und mehrere zentralisierte Server-Dienste realisiert. Sowohl das Protokoll als solches als auch die Architektur wurde durch die Firma Skype Inc. selbst nicht veröffentlicht. Dennoch konnte durch Analyse des Kommunikationsverhaltens die Architektur ermittelt werden [Baset & Schulzrinne 2006; Biondi & Desclaux].

Die Skype-Knoten sind in einer Superpeer-Architektur organisiert. Zusätzlich gibt es noch so genannte Login-Server, welche für die Authentifizierung zuständig sind, und dedizierte Systeme für die Anbindung von klassischen Telefonnetzen. Insofern handelt es sich um eine Superpeer-Architektur, die um zentrale Komponenten erweitert wurde. Wie der Skype-Ausfall im August 2007, bei dem es zu

[20] Für BitTorrent existieren zwei unabhängige DHTs: zum einen die in [BitT BEP5 2008] beschriebene "offizielle" Protokollerweiterung und zum anderen wird eine weitere DHT durch die BitTorrent-Implementierung Azureus [WWW Azureus] aufgespannt.

einer Überlastung der Login-Server kam, zeigt, ist ein Betrieb ohne die zentralisierten Login-Server nicht möglich (vgl. [Arak 2007]).

Bei Skype wird durch das P2P-System primär ein Nutzerverzeichnis realisiert, das zu einem gegebenen Skype-Namen die entsprechende aktuelle Netzwerkadresse (IP-Adresse und Port) liefert. Die Kommunikation zwischen Skype-Peers findet in der Regel direkt statt. Sollte eine direkte Verbindung zwischen zwei Knoten aufgrund von Firewalls oder NAT-Routern nicht möglich sein, können die Datenpakete auch über ein drittes Skype-Peer vermittelt werden.

Internet Indirection Infrastructure (i3)

Motivation für die *Internet Indirection Infrastructure (i3)* [Stoica et al. 2002] war die Tatsache, dass für die Internet-weite Realisierung von Mobilitätsunterstützung (Mobile-IP) sowie Multi- und Anycast-Diensten auf IP-Ebene die Unterstützung vieler Netzbetreiber notwendig wäre. Daher wurde durch i3 eine Indirektionsebene auf Anwendungsschicht eingeführt, die Sender und Empfänger entkoppelt und somit die Realisierung der genannten Punkte ermöglicht.

Die Kommunikation in i3 basiert auf so genannten Triggern. Die Trigger setzen sich entweder aus einer i3-spezifischen *ID* und einer Netzadresse (IP-Adresse und Port) zusammen oder verweisen auf einen weiteren Trigger. Ein Sender adressiert Datenpakete beim Senden nur mittels der *ID*. Auf einem i3-Knoten wird das Datenpaket an die nächste *ID* oder, falls der Trigger eine Netzadresse beinhaltet, an diese weiter geschickt. Ein Empfänger kann sich mittels eines Triggers für eine *ID* registrieren und somit lässt sich auch Multi- und Anycast realisieren.

i3 basiert auf dem P2P-Netz Chord. Die Trigger werden dabei in der DHT verwaltet und auch das Routing der Datenpakete findet über das Chord-Netz statt. Im Gegensatz zu den meisten anderen P2P-Systemen findet sämtliche Kommunikation, d.h. Weiterleitung der Datenpakete, mittels des P2P-Netzes statt.

CoralCDN

Durch *CoralCDN* [WWW Coral] wird ein P2P-System zur Verteilung von Web-Inhalten (engl. Content Distribution Network, CDN) zur Verfügung gestellt. Ziel des Systems ist es, Websites, die temporär hohe Popularität erreichen (engl. Flash Crowd oder auch Slashdot Effect genannt), zu entlasten und die Inhalte durch eine Reihe von HTTP-Proxies, so genannte CoralProxies, zugänglich zu machen. Die CoralProxies sind mittels einer DHT organisiert und stellen insofern die Knoten eines P2P-Netzes dar.

Um das System nutzbar zu machen, ohne Browser modifizieren zu müssen,

wird ein angepasster DNS-Server genutzt. Dieser weist dem anfragenden Client zunächst einen CoralProxy zu, welcher dem Client nahe ist. Der CoralProxy bildet dann aus der angefragten URL einen Hash, welcher als Schlüssel für die Abfrage eines Wertes in der DHT dient. Nur wenn die Inhalte in der DHT noch nicht verfügbar sind, wird eine Anfrage an den ursprünglich bereitstellenden Web-Server gestellt und der Inhalt dann unter dem entsprechenden Schlüssel in der DHT abgelegt [Freedman et al. 2004].

2.4.5 Bewertung

Ein wesentliches Merkmal von P2P-Netzen ist die Möglichkeit zur effizienten Suche nach Ressourcen. Die nachfolgende Kommunikation erfolgt in der Regel direkt zwischen den Peers. In den meisten Fällen wird das P2P-Netz daher nur zur Weiterleitung von Suchnachrichten genutzt. Für die direkte Kommunikation können bekannte Technologien eingesetzt werden. So wird bspw. für den Dateitransfer bei Gnutella HTTP-Protokoll genutzt [Eberspächer & Schollmeier 2005]. Somit stellt die Suchfunktionalität das wesentliche Unterscheidungsmerkmal dar.

Vergleich strukturierter und unstrukturierter P2P-Netze

Die Bewertung und Klassifizierung von P2P-Netzen kann anhand zahlreicher Kriterien erfolgen. Als funktionales Kriterium sind die unterschiedlichen Möglichkeiten zur Realisierung der Suchfunktion hervorzuheben. Der maßgebliche Unterschied zwischen unstrukturierten und strukturierten P2P-Netzen besteht darin, dass bei unstrukturierten Netzen die Suche unabhängig vom Routing der (Such-)Nachrichten ist und somit auch komplexe oder unscharfe Suchanfragen[21] ausgewertet werden können. Bei strukturierten Netzen beschränkt sich die Suche im Wesentlichen auf eine exakte Suche, d.h. die Suche erfordert explizite die Angabe eines Schlüssels. Eine unscharfe Suche, wie zum Beispiel mit Jokerzeichen, ist bei strukturierten Netzen im Allgemeinen nicht möglich (vgl. u.a. [Chawathe et al. 2003], [Wehrle et al. 2005, S. 85]).

Ein Vorteil bei der Suche in strukturierten Netzen besteht darin, dass der Wert zu einem Schlüssel garantiert gefunden wird[22], wenn es einen solchen Wert gibt. Außerdem können bei strukturierten Netzen Garantien hinsichtlich der Kosten (in Form der Nachrichtenanzahl) für die Suche und Wartung der DHT gegeben werden [Hellerstein 2003]. Im Gegensatz dazu bedeutet eine misslungene Suche in einem unstrukturierten Netz nicht zwangsläufig, dass es keine gesuch-

[21] Darunter kann sowohl eine Stichwortsuche (engl. Keyword Search) fallen als auch komplexere Suchschemata, wie sie bspw. durch SQL ausgedrückt werden können.

[22] Unter der Annahme, dass das Netz ausreichend stabilisiert ist.

te Ressource im P2P-Netz gibt, da durch die Beschränkung der Reichweite von Suchanfragen die passenden Ergebnisse unter Umständen nicht gefunden werden [Huebsch et al. 2003, S. 323].

Bewertungsmaßstäbe

Neben den genannten elementaren Unterschieden, variieren P2P-Netze in zahlreichen weiteren Gesichtspunkte, wie zum Beispiel der Anzahl von Nachrichten, die notwendig sind, um ein neues Peer zu integrieren, oder dem resultierenden Durchmesser des P2P-Netzes.

Eine Zusammenfassung solcher Klassifikationskriterien und Metriken findet sich in [Mischke & Stiller 2004] in Verbindung mit [Stiller & Mischke 2005]. Zu den genannten Kriterien zählen unter anderem: Durchmesser des P2P-Netzes, Bisektionsweite[23] des P2P-Netzes, Knotengrad hinsichtlich ein- und ausgehender Verbindungen und Symmetrie des Netzes.

Die Beurteilung, ob ein P2P-Netz für ein bestimmtes P2P-System geeignet ist oder nicht, kann letztlich nur mit Kenntnis des Anwendungsbereichs eines P2P-Systems durchgeführt werden. Hierzu geben die beiden oben genannten Arbeiten eine sehr gute Hilfestellung. Dies zeigt sich bspw. auch in [Castro et al. 2005], wo die Vor- und Nachteile von strukturierten und unstrukturierten P2P-Netzen kontrovers diskutiert werden.

Weitere Bewertungsmaßstäbe finden sich unter anderem in [Götz et al. 2005] und [Wehrle et al. 2005] oder auch den zusammenfassenden Arbeiten, die im folgenden Abschnitt kurz vorgestellt werden.

2.5 Weitere zusammenfassende Arbeiten

Die immense Anzahl an Veröffentlichungen (vgl. insofern auch Abschnitt 3.1.2) und entwickelter P2P-Systeme zeigen, dass es nicht einfach ist, den Themenbereich P2P in all seinen Facetten zu erfassen. Insofern kommt zusammenfassenden Arbeiten eine große Bedeutung zu. Im Folgenden wird eine Auswahl von zusammenfassenden Arbeiten präsentiert.

- Eine der ersten Veröffentlichungen und oft zitierte Arbeit stellt das von A. Oram editierte Buch *Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology* [Oram 2001] aus dem Jahr 2001 dar. In dem Buch werden einerseits verschiedene Systeme präsentiert und andererseits wurde auch versucht die Spezifika von P2P-Systemen und deren Erfolg zu ergründen.

[23] Die Bisektionsweite entspricht der minimalen Anzahl an Verbindungen, die entfernt werden müssen, so dass ein Netz in zwei Teile zerfällt.

- J. Crowcroft und I. Pratt zeigen in ihrer Arbeit *Peer to Peer: Peering into the Future* [Crowcroft & Pratt 2002] von 2002 strukturierende Elemente für den Bereich P2P auf und betrachten die Entwicklungen im historischen Kontext.

- In dem umfangreichen Technischen Bericht *Peer-to-Peer Computing* [Milojicic et al. 2002] aus dem Jahr 2002 erläutern Milojicic et al. die Kernkonzepte von P2P-Systemen und präsentieren entsprechende Systeme. Des Weiteren werden die Vor- und Nachteile von P2P-Systemen diskutiert. Die Arbeit zeichnet sich vor allem durch die zahlreichen Strukturierungselemente aus, die eine Einordnung bzw. Gegenüberstellung von P2P-Systemen zu klassischen verteilten Systemen deutlich erleichtern.

- S. Androutsellis-Theotokis und D. Spinellis geben in ihrer Arbeit *A Survey of Peer-to-Peer Content Distribution Technologies* [Androutsellis-Theotokis & Spinellis 2004] aus dem Jahr 2004 zunächst einen umfassenden Überblick über P2P-Systeme. Im zweiten Teil der Arbeit werden ausgewählte existierende P2P-Systeme vorgestellt und eine Einordnung anhand eines entwickelten Schemas hinsichtlich der Inhalteverteilung (engl. Content Distribution) vorgenommen.

- In dem Buch *Peer-to-Peer Systems and Applications (LNCS 3485)* [Steinmetz & Wehrle 2005a], das von R. Steinmetz und K. Wehrle herausgegeben wurde, präsentieren unterschiedliche Autoren in 33 Kapiteln eine grundlegende Einführung in den Themenbereich P2P. Gleichzeitig werden auch Forschungsfragen diskutiert und zahlreiche Referenzen gegeben.

- Der *RFC 4981: Survey of Research towards Robust Peer-to-Peer Networks: Search Methods* [RFC 4981] wurde von den Autoren J. Risson und T. Moors verfasst und im September 2007 durch die IETF als informeller Request for Comment (RFC) veröffentlicht. Neben der Darlegung von P2P-spezifischen Grundlagen und ausgewählten P2P-Systemen, zeichnet sich der RFC vor allem durch die umfangreiche Sammlung von 388 Referenzen aus. Von den gleichen Autoren wurde auch die Arbeit *Survey of research towards robust peer-to-peer networks: search methods* [Risson & Moors 2006] verfasst.

- Von E. Lua und J. Crowcroft et el. wurde eine zusammenfassende Arbeit mit dem Titel *A survey and comparison of peer-to-peer overlay network schemes* [Lua et al. 2005] verfasst, die im Jahr 2005 veröffentlicht wurde. Nach einer kurzen Einführung beschränkt sich die Arbeit auf eine Vorstellung und Vergleich von populären P2P-Netzen.

Neben den genannten Arbeiten existiert noch Vielzahl weiterer Werke wie zum Beispiel [Miller 2001], [Barkai 2001], [Moore & Hebeler 2001], [Fattah 2002] oder [Schoder et al. 2002], die jedoch größtenteils etwas veraltet und für eine breitere Zielgruppe bestimmt sind.

2.6 Zusammenfassung

Um das Potential von P2P-Systemen und -Netzen zu bestimmen, wurden in diesem Kapitel als Grundlage der Arbeit die Hintergründe, grundlegende Definitionen sowie ausgewählte P2P-Netze und -Systeme präsentiert.

Hinsichtlich des Ursprungs von P2P-Systemen hat sich gezeigt, dass zwei Entwicklungsstränge zu erkennen sind. Zum einen konnte der Bedarf an Overlay-Netzen und insbesondere auch an zusätzlichen Adressierungsmöglichkeiten aus Sicht von Rechnernetzen motiviert werden. Zum anderen ergaben sich aus dem Blickwinkel der verteilten Systeme verschiedene Gründe wie die höhere Skalierbarkeit im Vergleich zu Client/Server-Architekturen oder die Nutzung brachliegender Ressourcen, die zur Entwicklung von P2P-Systemen führten.

Ausgehend von existierenden Arbeiten wurde anschließend die Definition des Begriffs P2P-System vorgenommen. Ein P2P-System wurde als ein massiv verteiltes System auf Basis eines Rechnernetzes mit dem Ziel der gegenseitigen Nutzung von Ressourcen definiert. Darüber hinaus wurden die Begriffe P2P-Netz, P2P-Anwendung und P2P-Gemeinschaft in Form eines Dreiebenenmodells zueinander in Beziehung gesetzt. Aus der Abgrenzung von P2P-Systemen in Hinblick auf die beiden Gebiete Ad-hoc-Netze und Grid ging hervor, dass sich Teilaspekte zwar gleichen, jedoch auch elementare Unterschiede zum P2P-Bereich bestehen.

Der abschließende Teil des Kapitels bildete die Vorstellung von ausgewählten P2P-Systemen und -Netzen. So wurde insbesondere das Konzept von DHTs am Beispiel von Chord und Kademlia verdeutlicht. Kademlia wird aufgrund seiner Relevanz im Internet auch in den folgenden Kapiteln zur Illustration und Bewertung von Sachverhalten herangezogen. Zur weiteren Vertiefung fand zum Abschluss des Kapitels noch eine Vorstellung weiterer zusammenfassender Arbeiten statt.

Während in diesem Kapitel das historische Herkommen und die Grundlagen zu P2P-Systemen im Vordergrund standen, wird im folgenden Kapitel die gegenwärtige Bedeutung von P2P-Systemen sowie deren Charakteristika herausgearbeitet, woraus sich letztlich auch bislang ungelöste Herausforderungen ergeben.

3

Charakterisierung von P2P-Systemen

P2P-Systeme und -Netze erlangten im Laufe der letzten Jahre eine erhebliche Relevanz im Internet. Um die gegenwärtige Situation zu verdeutlichen, wird in diesem Kapitel der Verbreitungsgrad solcher Systeme und die Anzahl wissenschaftlicher Veröffentlichungen zum diesem Thema aufgezeigt. Anschließend werden Charakteristika gegenwärtiger P2P-Systeme und insbesondere auch das Einsatzspektrum dargestellt, wobei sowohl die Entwicklersicht als auch der betriebliche Aspekte berücksichtigt werden. Diese Charakterisierung zeigt zum einen die Stärken von P2P-Systemen und -Netzen auf. Zum anderen offenbart sie jedoch auch Fragestellungen, die einer weiteren Untersuchung in den folgenden Kapiteln bedürfen.

3.1 Relevanz der P2P-Technologie

Wie in kaum einem anderen Gebiet fand die Entwicklung und Untersuchung von P2P-Systemen seit jeher parallel sowohl "im Internet" als auch in der Forschung statt. Dabei wurden die Entwicklungen und Impulse, die von einem Gebiet ausgingen, auch wieder sehr schnell vom jeweils anderen aufgenommen. Insofern wird die folgende Bewertung der Relevanz der P2P-Technologie aus verschiedenen Blickwinkeln vorgenommen.

3.1.1 P2P-Systeme im Internet

P2P-Systeme haben mittlerweile eine große Verbreitung im Internet gefunden. Ein Indiz dafür ist das verursachte Datenvolumen in Backbone-Netzen [Sen & Wang 2002]. Messungen im Netz der Deutschen Telekom und weiteren Betreibern aus dem Jahr 2003 und 2004 zeigen, dass zwischen 50 % und 70 % des gesamten Datenverkehrs auf P2P-Anwendungen wie eDonkey oder BitTorrent zurückzuführen ist [Haßlinger 2005]. Auch die Studien [Ipoque 2006] und [Ipoque 2007] aus dem Jahr 2006 bzw. 2007 lassen erkennen, dass nach wie vor mehr als 50 % des Datenverkehrs durch P2P-Systeme bedingt ist. Einzig die genutzten P2P-Systeme haben sich verändert, so wird bspw. Gnutella kaum noch genutzt, während die Nutzung von BitTorrent stetig zunimmt.

Bei solchen Analysen bleibt zu berücksichtigen, dass die Klassifikation des Verkehrs in der Regel auf "Standard-Ports"[1] beruht (vgl. auch [Karagiannis et al. 2004]). Dies ist jedoch nicht in jedem Falle zielführend, da aktuelle Implementierungen, wie zum Beispiel die BitTorrent-Applikation µTorrent standardmäßig einen zufälligen Port auswählen (vgl. insofern auch die Messung zur BitTorrent-DHT in Abschnitt 4.2.4).

Neben dem verursachten Datenaufkommen gibt die Anzahl der Nutzer einen weiteren Eindruck, um die Relevanz der P2P-Technologie zu erkennen. Bereits Napster vermochte eine große Anzahl von Teilnehmern innerhalb einer kurzen Zeit zu begeistern (vgl. Abschnitt 2.2.1). Mehrere aktuelle Untersuchungen zeigen, dass mehrere Millionen Teilnehmer gleichzeitig Systeme wie BitTorrent oder eMule nutzen [Falkner et al. 2007; Steiner et al. 2007]. Darüber hinaus gibt es noch eine Reihe weiterer erfolgreicher P2P-Anwendungen wie PPLive [WWW PPLive] für Video-Streaming [Huang 2007] oder Skype zur Sprachtelefonie mit Millionen von Nutzern [Rossi et al.].

Die Nutzerzahlen verdeutlichen auch, dass P2P-Systeme keineswegs nur zum Dateitausch Verwendung finden. Vielmehr gibt es mittlerweile unterschiedlichste Anwendungsbereiche, in welchen P2P-Systeme erfolgreich eingesetzt werden (vgl. auch Abschnitt 2.4.4). Dies schließt mittlerweile auch die Steuerung von so genannten Botnets[2] ein (vgl. u.a. [Holz et al. 2008]).

Die eingangs erwähnte enge Verzahnung von Entwicklungen im Internet und der wissenschaftlichen Forschung zeigt sich unter anderem durch die Tatsache, dass wissenschaftliche Entwicklungen zügig wieder in bestehende Systeme integriert werden. So wurde sowohl BitTorrent als auch eMule [WWW eMule] um

[1] Für P2P-Systeme gibt es in der Regel keine Ports, die bei der IANA verzeichnet sind [IANA Ports]. Vielmehr führt die faktische Nutzung eines gewissen Ports in einer weit verbreiteten P2P-Anwendung zu einem "Standard-Port".

[2] Unter einem Botnetz versteht man eine Menge mit Schadsoftware infizierter Rechner, die ferngesteuert werden können.

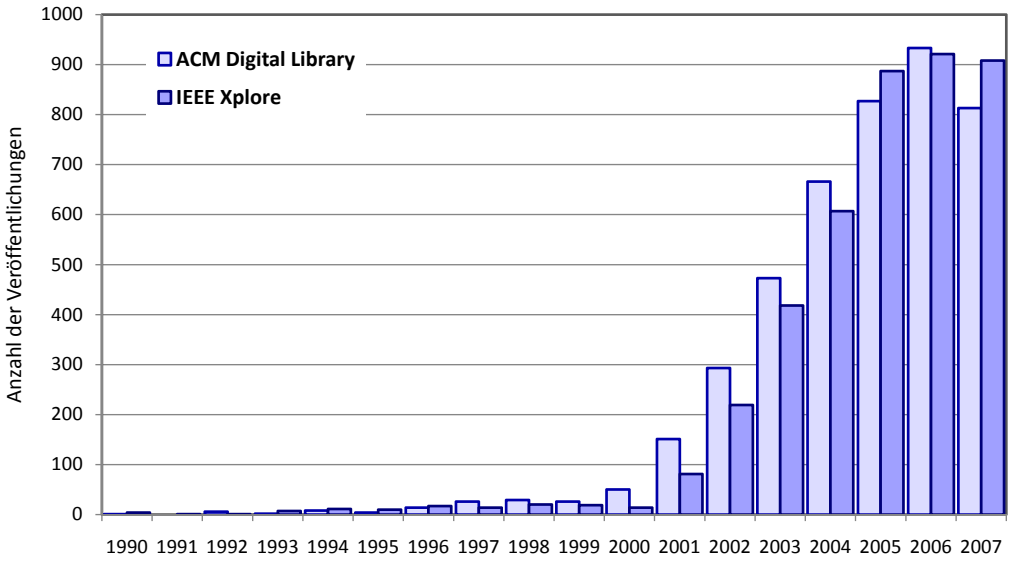


Abbildung 3.1: Anzahl der Veröffentlichungen im P2P-Bereich nach Jahren

eine auf Kademlia basierende DHT erweitert. Bei DHTs zeichnet sich insofern ein Trend hinzu Kademlia ab. Ferner gilt auch die DHT Bamboo [WWW Bamboo], die insbesondere bei OpenDHT zum Einsatz kommt, als robust und wurde ausreichend für den praktischen Einsatz optimiert [Rhea et al. 2005a]. Systeme wie Skype und Kazaa zeigen aber auch, dass auch Superpeer-Architekturen das Potential haben, Millionen von Nutzer zu unterstützen.

3.1.2 Wissenschaftliche Arbeiten

Der überaus große Nutzungsgrad von P2P-Systemen und die Breite des Themas führten zu einer großen Menge wissenschaftlicher Veröffentlichungen, wie sich an der Anzahl der Veröffentlichungen, die über das *ACM Portal* [WWW ACM Portal] und das *IEEE Xplore*-Portal [WWW IEEE Xpl] verfügbar sind, erkennen lässt.

In Abb. 3.1 ist die Anzahl der Veröffentlichungen in Abhängigkeit vom Jahr dargestellt. Die Zahlen wurden durch eine Suche mittels des Suchbegriffs “Peer-to-Peer” gewonnen[3]. Im Falle der *ACM Digital Library* wurden nur solche Arbeiten berücksichtigt, bei denen der Suchbegriff im Titel oder im Abstract enthalten war. Das IEEE Portal erlaubte zusätzlich eine Volltextsuche.

Die *ACM Digital Library* enthält Veröffentlichungen, von denen ACM Herausgeber oder zumindest Mitherausgeber ist. Beim IEEE-Portal wurden IEEE-Veröffentlichungen wie Bücher, Konferenzbände etc. berücksichtigt (vgl. [WWW

[3] Die Suche erfolgte jeweils am 10. März 2008.

IEEE Faq]). Die Ergebnisse sind daher weitestgehend disjunkt[4], so dass sich eine untere Grenze für die Gesamtzahl der Veröffentlichung durch Addition der Werte des IEEE-Portals und der ACM Digital Library ergibt.

Zählt man die Veröffentlichungen bei ACM und IEEE aus den Jahren 2000 bis 2007 zusammen, ergibt sich eine Summe von mehr als 8.000 Veröffentlichungen. Nimmt man noch die Veröffentlichung anderer Verlage wie Springer oder Elsevier hinzu, dürfte die Anzahl weit über 10.000 Veröffentlichungen liegen. Wie aus der Abb. 3.1 deutlich wird, gleicht sich der Trend in der Entwicklung der beiden ermittelten Werte. Die Verwendung des Begriffs "Peer-to-Peer" nimmt ab dem Jahr 2001 explosionsartig zu. Die Stagnation bzw. der leichte Rückgang der Veröffentlichungen im Jahr 2007 lässt vermuten, dass der Höhepunkt des "wissenschaftlichen Booms" überschritten ist.

Neben der Anzahl wissenschaftlicher Arbeiten im Bereich P2P nahm auch die Anzahl spezialisierter Konferenzen, Workshops und Symposien zu. Des Weiteren wurde das Thema von etablierten Konferenzen wie der *ACM Sigcomm Conference* oder der *Very Large Data Bases Conference (VLDB)* aufgegriffen. Eine vollständige Auflistung aller Konferenzen kann aufgrund der großen Menge an dieser Stelle nicht stattfinden. Vielmehr sollen zwei ausgewählte Veranstaltungen Erwähnung finden, die sich über Jahre hinweg etabliert haben. Dies ist zum einen *The IEEE International Conference on Peer-to-Peer Computing (IEEE P2P)* und zum anderen *The International Workshop on Peer-To-Peer Systems (IPTPS)*. Im Rahmen von ökonomischen Betrachtungen ist ferner der *Workshop on Economics of Peer-to-Peer Systems (P2PECON)* zu erwähnen. Eine Übersicht von Veranstaltungen mit dem Fokus P2P findet sich unter [WWW Cfp].

3.1.3 Standardisierungen

Eine Standardisierung von P2P-Systemen und insbesondere den darin enthaltenen P2P-Netzen fand bislang nicht statt. Vielfach werden proprietäre unveröffentlichte Protokolle wie bei Skype oder Kazaa verwendet. Teilweise werden zwar Protokollspezifikationen wie bei BitTorrent (vgl. [WWW BitT Dev]) veröffentlicht oder es erfolgt eine faktische Spezifikation, indem der Quelltext der P2P-Anwendung veröffentlicht wird. Dennoch fehlt eine verbindliche Standardisierung[5] von einer im Internet allgemein anerkannten Institution bzw. Gremium wie der IETF (Internet Engineering Task Force) oder dem W3C (Internet Engineering Task Force).

[4] Dies wurde auch durch einen weiteren Suchlauf mittels *ACM The Guide* bestätigt. Zusätzlich zu den Veröffentlichungen in der *ACM Digital Library* enthält *ACM The Guide* noch weitere Veröffentlichungen von mehr als dreitausend Herausgebern (vgl. [WWW ACM Faq]).

[5] vgl. zu Standardisierungen im Internet [Dinger & Hartenstein 2008, S. 60]

Ziel des von Sun Microsystems initiierten Projektes JXTA war es, P2P-Protokolle zu standardisieren [Gong 2001] (vgl. zu JXTA auch Abschnitt 4.1.2). Hierzu wurde sowohl eine Plattform als auch entsprechende Spezifikationen [JXTA Spec 2007] entwickelt. Sun Microsystems reichte die entwickelten Protokolle im Jahr 2002 bei der IETF ein. Im Rahmen der IETF hielt man die Standardisierung jedoch für verfrüht [Yeager & Bhattacharjee 2005] und gründete letztlich die *IRTF P2P Research Group* [WWW P2PRG], welche einerseits zum Ziel hat, Forschern eine Plattform zur Diskussion zu bieten und andererseits die Optionen für eine Standardisierung zu eruieren. So entstand insbesondere die zusammenfassende Arbeit [RFC 4981] von J. Risson und T. Moors (vgl. Abschnitt 2.5).

Im Jahr 2007 wurde die spezialisierte IETF Arbeitsgruppe P2psip [WWW P2psip] eingesetzt, deren Ziel es ist, die konventionelle Client/Server-Architektur, die dem Session Initiation Protocol (SIP) [RFC 3261] zugrunde liegt, um eine P2P-basierte Lösung zu ergänzen. Hierzu werden vor allem Lösungen auf Basis von DHTs diskutiert.

3.1.4 Bewertung und Trends

Aus den vorgenannten Aspekten lassen sich zusammenfassend folgende Bewertung und Trends ableiten:

- Die Verbreitung und der Einfluss von P2P-Systemen im Internet ist beträchtlich. Dies zeigt sich insbesondere im erzeugten Datenvolumen, der große Nutzerzahl sowie den vielfältigen Anwendungsbereichen.
- Mittlerweile zeichnet sich eine Konsolidierung hinzu wenigen Architekturen bzw. Protokollen (zum Beispiel Kademlia) ab, wie sie von J. Hellerstein in [Hellerstein 2003, S. 36] prophezeit wurde.
- Nach einer Phase intensiver Forschung scheint die Anzahl der Veröffentlichungen leicht rückläufig und der Zenit des P2P-Booms im wissenschaftlichen Bereich überschritten zu sein.
- Mittlerweile sind in ausgewählten Anwendungsbereichen greifbare Standardisierungsbemühungen erkennbar.
- Die P2P-Technologie entwickelt sich aufgrund der Konsolidierung einhergehend mit Standardisierungen mehr und mehr zu einer “Standardtechnik” (engl. Off-the-Shelf Technology) und ist somit auch zunehmend für klassische Anwendungsbereiche von verteilten Systemen, wie zum Beispiel Netzwerkmanagement [Granville et al. 2005; Pras et al. 2007] interessant.

3.2 Kernelemente und Rollen

Um das Potential der P2P-Technologie bewerten zu können, ist es notwendig, diese in den technischen Kontext einzuordnen. Hierzu bedarf es zunächst einer Identifikation von Kernelementen sowie Rollen.

3.2.1 Funktionale Kernelemente von P2P-Systemen

Auf funktionaler Sicht weisen P2P-Systeme drei Kernelemente auf:

1. *Suche* nach Ressourcen
2. *Routing* im P2P-Netz
3. Möglichkeiten zur *Ressourcennutzung*

Suche: Kernaufgabe von P2P-Systemen ist es, passende Ressourcen respektive Inhalte zu einer Suchanfrage zu finden. Für die Beantwortung der Suchanfragen bedarf es eines, gegebenenfalls verteilten, *Index*. Je nach System können folgende drei Arten an Indices unterschieden werden (vgl. [Risson & Moors 2006, S. 3489] und [Hellerstein 2003]):

- *Zentraler Index:* Bei hybriden Systemen wird der Index zentral vorgehalten und jedes Peer kennt die Adresse des zentralen Index. Die Peers teilen dem zentralen Index ihre verfügbaren Ressourcen mit. Somit kann eine Suchanfrage allein durch den zentralen Index beantwortet werden.

- *Lokaler Index:* Sind jedem Peer nur die eigenen Ressourcen bekannt, handelt es sich jeweils um einen lokalen Index. In der ersten Version von Gnutella war dies zum Beispiel der Fall. Die Suchanfrage wird dabei lokal ausgewertet und es findet insofern kein inhaltsbezogenes Routing der Suchnachricht statt. Teilweise werden diese lokalen Indices aggregiert wie in Superpeer-Architekturen oder zwischengespeichert wie in [Chawathe et al. 2003], um die Skalierbarkeit und Verfügbarkeit zu erhöhen.

- *Verteilter Index:* Bei einem verteilten Index werden die Indexeinträge nach einem festgelegten Verfahren auf die Peers verteilt. Typisches Beispiel hierfür sind die DHTs. Dabei erfolgt eine Zuweisung der Indexeinträge anhand der Knotenkennungen und durch das zugehörige Routing-Protokoll wird gewährleistet, dass die zuständigen Peers gefunden werden. Um Knoten zu entlasten bzw. die Verfügbarkeit zu erhöhen, werden Einträge in verteilten Indices teilweise auf mehrere Knoten repliziert oder auch zwischengespeichert (vgl. u.a. Kademlia [Maymounkov & Mazieres 2002]).

Routing: Die Suchfunktionalität in P2P-Systemen erfordert eine Weiterleitung von Suchnachrichten zu den passenden Indices. Je nach P2P-Netz kommen hierzu unterschiedliche Routing-Verfahren zum Einsatz. Dies reicht von einfachen Flut-basierten Ansätzen bis hin zu komplexeren Verfahren bei DHT-basierten P2P-Netzen. Für die Weiterleitung der Nachrichten wird in jedem Fall eine *Nachbarschaftstabelle* benötigt, die aus einer Liste bekannter Peers besteht. Gegebenenfalls erfolgt die Auswahl und Strukturierung der Knoten anhand der *P2P-spezifischen Kennungen*. Im Fall von hybriden Netzen setzt sich die Nachbarschaftstabelle lediglich aus der Adresse des zentralen Index-Servers zusammen. Bei Kademlia entspricht die Nachbarschaftstabelle den k-Buckets und bei Chord der Finger Table.

Regelmäßig ausgeführte Wartungsverfahren stellen sicher, dass die Nachbarschaftstabellen aktuell und funktionsfähig bleiben. Diese Verfahren werden teilweise auch als Stabilisierungsverfahren bezeichnet [Stoica et al. 2001] und prüfen insbesondere, ob die bekannten Peers noch verfügbar sind. Nicht mehr verfügbare Peers werden entfernt und passende neue Peers ergänzt. Die Regelmäßigkeit ergibt sich durch ein spezifiziertes *Aktualisierungsintervall* und die Überprüfung der Peers findet durch so genannte Ping-Pakete statt, daher wird im weiteren Verlauf der Arbeit hierfür auch der verkürzende Ausdruck "Ping-Rate" gebraucht. Zudem werden je nach Routing-Verfahren auch Peers ausgetauscht, wenn im Sinne der Routing-Metrik passendere Peers aktiv sind. Bei einigen P2P-Netzen, wie zum Beispiel Kademlia kann die Wartung in Teilen auch passiv erfolgen, indem die aus Suchanfragen bekannten Peers berücksichtigt werden.

Das Routing in P2P-Netzen ist insofern vergleichbar mit klassischem IP-Routing, bei welchem einerseits eine Weiterleitung von IP-Paketen anhand einer Routing-Tabelle stattfindet und andererseits parallel Routing-Protokolle wie OSPF genutzt werden, um die Routing-Tabelle aufzubauen und aktuell zu halten (vgl. zu IP-Routing u.a. [Aweya 2001])[6]. Teilweise wird die Nachbarschaftstabelle daher als *Routing-Tabelle* bezeichnet.

P2P-Systeme sind Daten-zentrisch (engl. Data-Centric), so dass der Fokus beim Routing auf dem Inhalt selbst und nicht auf dem unterliegenden, bereitstellenden System liegt. Im Unterschied zum IP-Routing, dessen Ziel es ist, Datenpakete einem bestimmten System zuzustellen, handelt es sich bei P2P-Netzen um ein inhaltsbezogenes Routing (engl. Content-based Routing) bzw. inhaltsbasierte Adressierung (vgl. zu inhaltsbezogenem Routing [Carzaniga & Wolf 2002]). Im Fall von DHTs spricht man aufgrund der Schlüssel/Wert-Paare auch von *Key-based Routing (KBR)* [Dabek et al. 2003].

[6] Fluten ist insofern bei IP vergleichbar mit einer Broadcast bzw. Multicast-Kommunikation.

Ressourcenzugriff / Inhalteverteilung: Der eigentliche Ressourcenzugriff gestaltet sich häufig simpel, da lediglich eine direkte Verbindung zwischen dem bzw. den anbietenden und dem konsumierenden Peer aufgebaut wird. Die Protokolle, um auf eine Ressource bzw. Inhalt wie eine Datei zu zugreifen, sind daher meist unabhängig vom Routing-Protokoll und es kommen häufig etablierte Protokolle wie das HTTP-Protokoll zum Einsatz (vgl. u.a. [Eberspächer & Schollmeier 2005, S. 41]). Werden Inhalte von mehreren Knoten gleichzeitig bezogen wie bei BitTorrent, muss eine passende Segmentierung und Reassemblierung stattfinden.

Anders stellt sich die Situation bei Systemen wie i3 oder anderen Multicast-Systemen dar. Bei solchen Systemen werden alle Datenpakete bei der Ressourcennutzung mittels eines oder mehrerer *dritter* Peers[7] weitergeleitet. Eine weitere Ausnahme bilden Anonymisierungsdienste, bei welchen der Ressourcenzugriff P2P-spezifische Routing-Verfahren nutzt, so dass die Identität von Sender bzw. Empfänger verschleiert wird.

3.2.2 Rollenverteilung in P2P-Systemen

Im Kontext von P2P-Systemen können drei Rollen unterschieden werden, wobei von ein und derselben Person bzw. Organisation mehrere Rollen wahrgenommen werden können:

- *Entwickler:* Die Spezifikation von P2P-Kommunikationsprotokollen und Realisierung entsprechender Anwendungen (auch als P2P-Client bezeichnet) wird von der Rolle Entwickler wahrgenommen. Da in der Regel keine Standardisierung stattfindet, legt der Anwendungsentwickler zugleich das Kommunikationsprotokoll fest. Trotz fehlender Standardisierung können bei offenen Systemen wie BitTorrent unterschiedliche P2P-Clients implementiert werden, die zueinander hinsichtlich des Kommunikationsprotokolls kompatibel sind. In dem Falle sind Hauptentwickler, die auch das Kommunikationsprotokoll definieren, von anderen Entwicklern zu unterscheiden.

- *Betreiber:* Jeder Teilnehmer eines P2P-Systems ist zugleich auch Betreiber. Bei Betreibern von P2P-Systemen ist danach zu differenzieren, ob das P2P-System nur aus gleichartigen Peers besteht oder ob zusätzliche Komponenten bzw. Dienste zum Einsatz kommen, die für den Betrieb des Systems unerlässlich sind und nur von *einem* Betreiber betrieben werden.

  - *Exponierter Betreiber:* Kommen zusätzliche, zentrale Komponenten eines Betreibers zum Einsatz, gibt es einen herausgestellten Betreiber

[7] Diese werden auch als *Rendezvous Peers* bezeichnet

neben einer Menge von Peer-Betreibern. So betreibt Skype bspw. in Form der Login-Server solche Komponenten und ist insofern ein exponierter Betreiber.

- *Menge von Betreibern:* Sind alle Peer-Betreiber grundsätzlich gleich und somit beliebig austauschbar, handelt es sich um eine Menge von Betreibern.

– *Nutzer:* Jeder Teilnehmer eines P2P-Systems ist in der Regel auch Nutzer, da die Rollen symmetrisch verteilt sind (vgl. auch Abschnitt 2.3.1).

3.3 Einordnung und Bewertung der P2P-Technologie

Ziel diese Abschnittes ist es, eine Einordnung und Bewertung der gegenwärtigen P2P-Technologie vorzunehmen. Zunächst wird hierzu eine Einordnung im Kontext von Rechnernetzen und verteilten Systemen vorgenommen. Im zweiten Unterabschnitt wird dann die essenzielle Rolle der Dezentralität diskutiert. Abschließend werden resultierende Eigenschaften von gegenwärtigen P2P-Systemen dargelegt.

3.3.1 P2P eine Virtualisierungstechnik

Teilweise argumentieren Autoren wie zum Beispiel in [Minar & Hedlund 2001, S. IX], dass P2P-Systeme das "klassische Internet" wieder "zurückbringen", welches sich durch die Einführung von dynamischen IP-Adressen und die Kommunikation über NAT-Router sowie das Client/Server-Architekturmuster gewandelt hat.

Diese Argumentation beinhaltet zwei unterschiedliche Aspekte, die einer gesonderten Betrachtung bedürfen. Dies ist zum einen die Sicht auf P2P-Systeme als Fortentwicklung bzw. Teil von Rechnernetzen und zum anderen aus Sicht von verteilten Systemen (vgl. insofern auch Abschnitt 2.1). Die Sinnhaftigkeit sich der Thematik von beiden Seiten – Top-Down und Bottom-Up – zu nähern, wird auch durch die Beobachtung gestützt, dass die Unterscheidung von Anwendungsschicht und Netzwerkschicht zunehmend schwieriger wird [Peterson & Davie 2003, S. 680][8]. Insofern erfolgt die folgende Betrachtung auch aus beiden Perspektiven.

[8] Aus diesem Grund wird teilweise auch in Frage gestellt, ob das Schichtenmodell für die Modellierung von künftigen Netzwerkarchitekturen geeignet ist [Clark 2005].

Aus Sicht von Rechnernetzen: Aus Sicht der Rechnernetze sind P2P-Systeme vor allem durch ihre Eigenschaft als Overlay-Netz geprägt, wobei P2P-Netze im Vergleich zu anderen Overlay-Netzen wie virtuellen privaten Netzen selbstorganisierend sind. Durch P2P-Netze werden neue, zusätzliche Adressräume eröffnet, die eine Ende-zu-Ende-Kommunikation wieder ermöglichen, die durch IP-Adressen nicht mehr in jedem Falle gegeben ist. Die Funktionalität wurde dabei in für das Internet typischer Weise "am Rand" ergänzt[9] und nicht im Kern des Netzes wie IP-Routern integriert (vgl. auch [Steinmetz & Wehrle 2005a, S. 10]).

In Teilen sind P2P-Netze vergleichbar mit *virtuellen lokalen Netzen* (engl. Virtual LAN, VLAN) auf Basis von Ethernet[10], die auch ein zusätzliches Adressierungselement einführen. Bei beiden ist es möglich virtuelle Netze zu formen, die nicht an physikalische bzw. örtliche Einschränkungen gebunden sind. Vielmehr kann die Auswahl der Netzteilnehmer auf einer rein logischen Ebene unter funktionalen Gesichtspunkten erfolgen. Weiterhin sind beide Netzarten dadurch geprägt, spezialisierte Netze für eine bestimmte Gruppe bzw. Einsatzzweck zu etablieren. Im Unterschied zu P2P-Netzen sind VLANs allerdings nicht selbstorganisierend.

Aus Netzsicht können P2P-Netze insofern auch als *Virtualisierungstechnik* verstanden werden, die eine Entkopplung vom unterliegenden Netz, in der Regel dem Internet und dessen IP-Protokoll, erlauben.

Aus Sicht von verteilten Systemen: Aus dem Blickwinkel von verteilten Systemen betrachtet, zeichnen sich P2P-Systeme durch die symmetrische Rollenverteilung aus, bei welcher die Peers sowohl die Rolle als Dienstgeber als auch Dienstnehmer einnehmen können. Dies unterscheidet P2P-Systeme vom Client/Server-Architekturmuster auf Rechnerebene. Dennoch bringen P2P-Systeme nicht, wie von anderen Autoren artikuliert, das "klassische Internet zurück". Vielmehr hat sich eine Systemkategorie entwickelt, die den Aufbau von massiv verteilten Systemen in effizienter Weise erlaubt, wobei die Komponenten des verteilten Systems wiederum selbst Informationssysteme darstellen können.

Zu Beginn des Internet gab es nur wenige (Groß-)Rechner und die Nutzer interagierten mit diesen Rechnern direkt mittels Terminals. Kurz, es gab nur wenige Server, deren Adressen wohlbekannt waren. Im Laufe der 1990er Jahre erhöhte sich die Anzahl der Rechner massiv durch die hinzu kommenden PCs. Gleichzeitig fand auch eine Umsetzung des Client/Server-Paradigmas auf Rechnerebene statt (vgl. auch Abschnitt 2.1.1). Insofern fand keine Trennung in Client und Server auf Basis der bestehenden Rechnermenge statt. Vielmehr kam eine

[9] vgl. das *End-to-End Argument* in [Saltzer et al. 1984] und bspw. die Realisierung des Domain Name System (DNS) [Mockapetris & Dunlap 1995]

[10] vgl. zu VLANs unter anderem [Dinger & Hartenstein 2008, S. 33] oder [Halsall 2005, S. 195 ff]

große Anzahl von Rechnern, die Clients, hinzu. Dabei führte die Anwendung des Client/Server-Paradigmas zu einer Strukturierung der Rechnermenge sowie Reduktion der notwendigen wohlbekannten Adressen, da nur die Server-Adressen wohlbekannt sein müssen.

Um einerseits der zunehmenden Komplexität zu begegnen und andererseits der geforderten Flexibilität gerecht zu werden, wurden die Architekturen zunehmend modularer. Bei verteilten Systemen wurde mittels so genannter Multi-Tier-Architekturen insbesondere die Applikationslogik von den Ressourcen getrennt (vgl. auch Abschnitt 4.1.2). Im Gegensatz zu dieser funktionalen Separierung ermöglichen P2P-Systeme insbesondere eine Verteilung der Last auf viele Systeme. Durch P2P-Systeme wird eine logische Schicht geschaffen, die von konkreten Rechnersystemen abstrahiert und (in der Regel selbstorganisierend) eine Aufteilung der Last ermöglicht.

Insofern wird durch P2P-Systeme die Anwendung vom Rechnersystem entkoppelt und auch aus Sicht der verteilten Systeme kann das P2P-Paradigma als *Virtualisierungstechnik* aufgefasst werden. Letztlich eröffnen P2P-Systeme somit die Möglichkeit, Attribute die typischerweise mit dem Internet assoziiert werden, wie die Robustheit gegenüber Fehlern und die Skalierbarkeit hinsichtlich der Teilnehmerzahl, auf den Bereich der verteilten Systeme zu übertragen.

3.3.2 Dezentralität von P2P-Systemen

Dezentralität ist sowohl bei P2P-Gemeinschaften als bei P2P-Systemen ein fundamentales Konzept. Indem die Bedeutung von zentralen Entitäten reduziert wird, wird auch die Monopolbildung und Zensur erschwert, wenn nicht gar komplett verhindert [Agre 2003].

> *"P2P delivers on the Internet's promise of decentralization."*
> von P. Agre [Agre 2003, S. 39]

Aus technischer Sicht hat eine dezentrale Struktur das Potential, durch die Vermeidung von Single-Point-of-Failures, die Robustheit gegenüber Ausfällen zu erhöhen und skalierbar zu sein. Dabei sei angemerkt, dass der Rückschluss, d.h. eine dezentrale Architektur ist skalierbar und robust, im Allgemeinen nicht erfüllt ist. Die Unabhängigkeit von zentralen Infrastrukturen bzw. die Funktionsfähigkeit des Netzes beim Ausfall einzelner Teile stellt auch ein zentrales Konzept des Internet dar [Clark 1988].

Der Grad der Dezentralität ist je nach P2P-System verschieden. Ferner ist die Dezentralität auch nicht für alle Funktionen eines P2P-Systems in gleichem Maße gegeben. Im Folgenden wird daher eine differenzierte Betrachtung der Dezentra-

lität von P2P-Systemen vorgenommen. Abgeleitet von den elementaren Funktionen, ergeben sich folgende Parameter:

- *Ressourcenlokationen:* Die Anzahl der Orte bzw. Systeme, an welchen sich Ressourcen befinden, wird mittels des Parameters *Ressourcenlokationen* loc zum Ausdruck gebracht. Gemäß der Definition von P2P-Systemen sind die Ressourcen bzw. Inhalte selbst immer verteilt, d.h. dezentral verfügbar. Zur Vereinfachung wird für die folgenden Betrachtungen angenommen, dass jedes Peer genau eine Ressource vorhält und somit die Anzahl der Ressourcenlokationen der Knotenzahl entspricht.

- *Index:* Zur Beantwortung von Suchanfragen wird bei P2P-Systemen ein Index genutzt (vgl. Abschnitt 3.2.1). Der *Index*-Parameter $\mathrm{idx} = (\mathrm{i} : \mathrm{j})$ drückt das Verhältnis zwischen Index und Ressourcen aus. Dabei entspricht i der Anzahl der Knoten, welche an der Verwaltung des Index beteiligt sind, d.h. im Falle von lokalen Indices deren Anzahl und bei einem verteilten Index wie bei DHTs der Anzahl beteiligter Knoten. Durch j wird ausgedrückt, auf wie viele Ressourcenlokationen *ein* Index (bzw. *ein* Teil eines Indexes bei einem verteilten Index) durchschnittlich verweist.

- *Entitäten zur ID-Vergabe:* Der Parameter *Entitäten zur ID-Vergabe* eid entspricht der Anzahl Entitäten, welche P2P-spezifische Kennungen vergeben. Kommen keine speziellen Kennungen zum Einsatz, wird dies gleichgesetzt mit: Jedes Peer kann selbst eine Kennung generieren. Dieser Parameter drückt letztlich auch die organisatorische Struktur des Systems aus und gibt an, ob es einen exponierten Betreiber gibt[11].

In Tabelle 3.1 sind die Parameter für verschiedene P2P-Systeme angegeben. Dabei entspricht n der Anzahl der Knoten. Ferner sei s die Anzahl der Knoten einer Teilmenge, so dass gilt $1 < \mathrm{s} < \mathrm{n}$. Zu Vergleichszwecken wurden auch klassische verteilte Systeme und das IP-Routing-Protokoll OSPF, das auch P2P-typische Eigenschaften aufweist, aufgenommen. Die Werte sind dabei in einer O-Notation-ähnlichen Schreibweise angegeben, d.h. konstante, von der Knotenanzahl unabhängige Faktoren werden vernachlässigt und mit einem Wert von 1 angegeben. Insofern können auch bei einem $\mathrm{i} = 1$ mehrere wohlbekannte Index-Server existieren.

In Hinblick auf die Dezentralität ist sowohl bei Ressourcenlokationen als auch der ID-Vergabe ein Parameterwert von n anzustreben. Im Sinne eines möglichst

[11] Durch Delegation kann auch eine Hierarchie von verwaltenden Entitäten geschaffen werden, wie dies bspw. bei der IP-Adressvergabe der Fall ist (vgl. u.a. [Dinger & Hartenstein 2008, S. 115]). Dennoch würde man auch bei einer Hierarchie von einem exponierten Betreiber sprechen.

System	**Ress.-Lok.** loc	**Index** idx	**ID-Vergabe** eid
Browser und ein Web-Server	1	$1:1$	1
VoIP mittels SIP-Server	n	$1:n$	1
OSPF	n	$n:n$	1
Napster	n	$1:n$	1
Gnutella 0.4	n	$n:1$	n
Gnutella 0.6	n	$s:\frac{n}{s}$	n
		$(1 << s << n)$	
Skype	n	$s:\frac{n}{s}$	1
		$(1 << s << n)$	
Internet Indirection Infrastructure (i3)	n	$n:1$	n
BitTorrent (mit Tracker)	n	$1:n$	n
BitTorrent (Trackerless)	n	$s:\frac{n}{s}$	n
	n	(1<<s<n)	

Tabelle 3.1: Einordnung von typischen P2P-Systemen und "klassischen Systemen" hinsichtlich Dezentralität

dezentralen Systems sollte ein Index-Parameter von $idx = (n : 1)$ anvisiert werden, so dass alle Knoten an der Verwaltung des Index beteiligt sind, aber jeder Knoten nur für eine konstante Anzahl Ressourcenlokationen zuständig ist.

Soll die Erreichbarkeit aller Ressourcen ermöglicht werden, muss die Invariante $loc \leqslant i \cdot j$ gelten. Dabei ist zu beachten, dass der Rückschluss, bei Erfüllung der Invariante seien alle Ressourcen erreichbar, nicht gilt wie sich bei Gnutella 0.4 zeigt.

Betrachtet man ein System bestehend aus einem Web-Server und Browser, ist augenfällig, dass alle Funktionen auf dem Web-Server konzentriert sind und sich somit alle Parameter zu 1 ergeben. Im Falle einer VoIP-Kommunikation, bei welcher der Verbindungsaufbau gemäß des SIP-Protokolls erfolgt, bestehen die Ressourcen aus allen potentiellen Gesprächsteilnehmern. Für die Verwaltung der SIP-Adressen ist nur eine konstante Anzahl SIP-Server zuständig, so dass $i = 1$ und $j = n$ gilt. Auch die Vergabe der SIP-Adressen ist zentralisiert und somit gilt $eid = 1$. Bei OSPF müssen die IP-Adressen der Router eindeutig vergeben sein ($eid = 1$). Jeder Router führt dabei eine Routing-Tabelle, so dass $i = n$ gilt. Da es sich bei OSPF um ein Link-State-Protokoll handelt und jeder Knoten somit eine komplette Sicht des Netzes hat, ergibt sich $j = n$.

Der Index bei Napster ist zentralisiert, so dass $idx = (1 : n)$ gilt. Ferner wird der Index auch für die Verwaltung der Kennungen ($eid = 1$) genutzt. Bei der Gnutella 0.4 kennt jedes Peer lediglich die selbst zur Verfügung gestellten Datei-

en, d.h. es gibt n lokale Indices und jeder lokale Index verweist jeweils auf *eine* Ressourcenlokation, so dass für den Index-Parameter $n : 1$ gilt. Spezifische P2P-Kennungen gibt es bei Gnutella nicht, daher ist $eid = n$. Bei einer Superpeer-Architektur wie Gnutella 0.6 werden Suchanfragen nur noch von einer beschränkten Menge Superpeers s beantwortet. Daher ergibt sich der Index-Parameter zu $idx = (s : \frac{n}{s})$, wobei s wesentlich kleiner als n ist. Skype realisiert auch eine Superpeer-Architektur, vergibt die P2P-spezifischen Kennungen jedoch durch dedizierte Login-Server [Baset & Schulzrinne 2006]. Außer dem Parameter $eid = 1$, sind die Parameter von Skype daher gleich denen von Gnutella 0.6.

Das P2P-System i3 nutzt Chord als unterliegendes P2P-Netz, was wiederum einen verteilten Index mittels einer DHT aufbaut. Die Knotenkennung kann dabei von jedem Peer selbst berechnet werden, so dass $eid = 1$ gilt. Bei i3 sind alle Knoten an der Verwaltung des verteilten Index beteiligt, wobei jeder Knoten für durchschnittlich $\frac{1}{n}$ des Schlüsselraums. Da n Peers existieren ergibt sich $j = n \cdot \frac{1}{n} = 1$.

Bei BitTorrent sind der *Trackerless-* und der *Tracker-Modus* zu differenzieren. Kommt ein Tracker zum Einsatz, ist die Funktionsweise hinsichtlich Dezentralität vergleichbar dem Napster-System, da der Index von einem Tracker verwaltet wird. Im Gegensatz zu Napster kommen jedoch mehrere Tracker zum Einsatz, was sich jedoch aufgrund der O-Notation-ähnlichen Schreibweise nicht auf den Parameter i auswirkt. Im Fall des Trackerless-Betriebs bauen die Peers eine DHT auf, die zur Verwaltung des Index genutzt wird. Es nehmen nicht zwangsläufig alle aktiven BitTorrent-Knoten an der DHT teil, daher ergibt sich ein Index-Parameter von $idx = (s : \frac{n}{s})$. Die P2P-spezifische Kennung wird von jedem Peer selbst gewählt ($eid = n$).

Die Betrachtung zeigt, dass die Dezentralität von P2P-Systemen unterschiedlich ist und einige Systeme wesentliche zentrale Komponenten enthalten. Hinsichtlich der Dezentralität sind die Parameter von DHTs wie i3 optimal, da alle Knoten an der Verwaltung des Index beteiligt sind und jeder Knoten nur für konstante Anzahl Ressourcenlokationen zuständig ist. Andererseits zeigt sich, dass auch Gnutella 0.4 optimale Parameter aufweist und insofern ein dezentrales P2P-System nicht in jedem Fall skalierbar ist.

Darüber hinaus bleibt zu beachten, dass für den Beitritt zu P2P-Systemen in der Regel eine zentrale Entität, ein so genannter *Bootstrap-Server*, zum Einsatz kommt (vgl. auch Abschnitt 4.2). Dies hat zwar keine Auswirkung auf die Dezentralität des P2P-Systems selbst, unter Einbezug des Betriebskontextes stellt dies jedoch eine wesentliche Einschränkung dar, da es das Wesen von P2P-Systemen ist, dass ein ständiger Peer-Wechsel, d.h. Churn, stattfindet (vgl. Abschnitt 2.3.1) und ein Bootstrap-Server eine elementare zentrale Komponente darstellt.

3.3.3 Eigenschaften von P2P-Systemen

Zusammenfassend ergeben sich für P2P-Systeme idealerweise folgende Eigenschaften, wobei zu berücksichtigen bleibt, dass nicht alle Eigenschaften auf alle P2P-Systeme gleichermaßen zutreffen.

- *Skalierbarkeit* – Die dezentrale Realisierung in Kombination mit selbstorganisierenden Verfahren führt dazu, dass die Bereitstellung der Ressourcen sowie die Verwaltung und Suchfunktionalität des P2P-System von den Peers selbst realisiert wird. Insofern ist ein solches System *selbstskalierend* hinsichtlich der Teilnehmerzahl [Chawathe et al. 2003, S. 407], da durch mehr Teilnehmer zwar mehr Last induziert wird, aber auch gleichzeitig mehr Ressourcen zur Verfügung stehen. Allerdings ist die Skalierbarkeit nur gegeben, solange neue Knoten im Durchschnitt nicht mehr Ressourcen nutzen als sie selbst bereitstellen.

  Aus wissenschaftlicher Sicht wurde die Skalierbarkeit vor allem im Bereich von DHTs nachgewiesen. Aus praktischer Sicht zeigt sich die Skalierbarkeit in einem gewissen Maße bereits durch die Millionen von Teilnehmern.

- *Robustheit* – Dezentrale Kontrolle, Adaptivität und die Fähigkeit zur Selbstorganisation führen schließlich dazu, dass P2P-Systeme robust gegenüber Fehlfunktionen von Knoten bzw. unvorhergesehenen Knotenausfällen sind (vgl. u.a. [Balakrishnan et al. 2003]). Wie im folgenden Abschnitt noch näher ausgeführt wird, ist damit aber die Robustheit hinsichtlich Angriffen nicht gegeben.

- *Autonomie* – Durch P2P-Systeme lassen sich autonome Systeme (vgl. zu Autonomie u.a. [Jaeger et al. 2008]) realisieren, in welche neue Peers ohne manuelle Konfiguration integrierbar sind und die adaptiv auf Ausfälle reagieren. Sie stellen somit eine Entwicklungsstufe hinzu dem, von der Firma IBM anvisierten, *Autonomic Computing* [Kephart & Chess 2003] und dessen Selbst-X-Eigenschaften (engl. Self-X) wie Selbst-Konfiguration, Selbst-Optimierung, Selbst-heilend und Selbst-schützend dar.

- *Kosteneffizienz* – Ein P2P-System ermöglicht eine Nutzung von vorhandenen Ressourcen, wie zum Beispiel PCs von Endanwendern, die ansonsten brach liegen würden, da sie nicht effizient für ein verteiltes System nutzbar wären. Insbesondere um Lastspitzen abzufedern, bieten sich P2P-Systeme an, wie in Abschnitt 2.4.4 anhand von CoralCDN dargestellt wurde. Aber auch im Falle einer gleichbleibenden Last kann sich ein P2P-System für exponierte Betreiber lohnen, wie das Beispiel Skype zeigt, da ein Teil der Betriebskosten von den Nutzern selbst übernommen wird.

– *Innovationspotential* – Die immense Anzahl existierender P2P-Systeme, die unterschiedlichsten Anwendungsbereichen entstammen, verdeutlicht welches Innovationspotential P2P-Systemen innewohnt. Die Realisierung von Overlay-Netzen auf Anwendungsebene ermöglicht es, Anwendungen, wie zum Beispiel Multicast-Applikationen zu entwickeln ohne die unterliegende Netzinfrastruktur ändern zu müssen. Insofern erweist sich wie bei anderen Systemen im Internet auch die Realisierung entsprechend des Ende-zu-Ende-Arguments auf Anwendungsschicht als innovationsfördernd (vgl. insofern auch [v. Schewick 2005]).

3.4 Identifikation von Herausforderungen unter Berücksichtigung betrieblicher Faktoren

Die Bewertung des Potentials von P2P-Netzen und -Systemen erfordert neben der Berücksichtigung von Entwicklungsaspekten auch eine Würdigung betrieblicher Faktoren. Dabei ist vor allem der Anwendungsbereich von P2P-Systemen, die Robustheit der Systeme gegenüber Angriffen sowie deren juristische Einordnung fraglich.

3.4.1 Horizontale Integration von P2P-Techniken in verteilten Systemarchitekturen

Wie sich aus obiger Darstellung ergibt, eignen sich P2P-Systeme für zahlreiche Anwendungsbereiche. Da diese Systeme in der Regel für dedizierte Aufgaben wie den Dateitausch entwickelt wurden, handelt es sich bei fast allen P2P-Systemen um vertikal integrierte Systeme, d.h. es werden keine standardisierten Protokolle und Schnittstellen eingesetzt [Androutsellis-Theotokis & Spinellis 2004, S. 338]. Vielmehr werden für jeden Anwendungsbereiche spezifische Komplettlösungen geschaffen, die in der Regel mittels einer monolithischen Architektur realisiert werden.

Somit ist auch keine Integration mit anderen verteilten Systemen, insbesondere Middleware-Architekturen (vgl. auch Abschnitt 4.1.2), gegeben. In einigen Anwendungsbereichen können P2P-Systeme zwar als eigenständige Systeme realisiert werden. Um P2P-Techniken jedoch effizient in komplexen Szenarien wie einem elektronischen Marktplatz nutzen zu können, bedarf es einer Integration in klassischen Systemarchitekturen, insbesondere aus dem Bereich der verteilten Systeme.

In der evolutionären Weiterentwicklung des P2P-Paradigmas wird daher eine

Integration in bestehende Architekturen verteilter Systeme gefordert sein. Insofern stellt sich die Frage, inwieweit eine (horizontale) Integration[12] von P2P-Techniken im Rahmen von komplexen verteilten Systemen möglich und sinnvoll ist.

3.4.2 Realisierung von Mikro-P2P-Systemen

Die Eignung von P2P-Systemen für Millionen von Teilnehmer und insbesondere deren Skalierbarkeit wurde sowohl in wissenschaftlichen Studien als auch durch existierende Systeme eindrucksvoll dargelegt (vgl. Abschnitt 3.1.1). Neben der Skalierbarkeit weisen P2P-Systeme aber auch andere Attribute auf wie die Ausfallrobustheit, die sich aus der Adaptivität der Systeme ergibt.

Von diesen Merkmalen könnten auch P2P-Systeme mit wenigen Teilnehmern, die im Folgenden als *Mikro-P2P-Systeme* bezeichnet werden, profitieren. Problematisch dabei ist, dass eine vollständige Dezentralität bei P2P-Systemen selbst zwar realisierbar ist, aber beim Aufbau eines P2P-Systems in der Regel zentralisierte Bootstrap-Server zum Einsatz kommen (vgl. u.a. [Cramer et al. 2004]). Dadurch bleibt fraglich wie die P2P-Technologie ihr Potential bei Mikro-P2P-Systemen entfalten kann, da vor allem bei kleinen Systemen solch ein zusätzlicher zentraler Server die Sinnhaftigkeit des Ganzen in Frage stellt.

3.4.3 Robustheit von P2P-Systemen unter dem Einfluss von gezielten Angriffen

P2P-Systeme werden häufig mit Attributen wie Robustheit und Skalierbarkeit assoziiert. Die Robustheit wird dabei im Wesentlichen durch Replikation von Daten und alternativen Routen sowie die Adaptivität der Systeme erreicht. Im Allgemeinen ist jedoch einzuschränken, dass die Robustheit nur hinsichtlich (einzelner) ausfallender Knoten gegeben ist und nicht zwangsläufig hinsichtlich böswilliger Knoten, die ein System gezielt angreifen.

> *"P2P is potentially a disruptive technology with numerous applications, but this potential will not be realized unless it is demonstrated to be robust."*
> von J. Risson und T. Moors [Risson & Moors 2006, S. 3486]

Das Potential von P2P-Systemen kann sich aber nur vollständig entfalten, wenn die Systeme sich auch als robust gegenüber Attacken erweisen. Dies gestaltet sich jedoch in einem offenen System ohne zentrale technische oder organisatorische

[12] Unter horizontalen Protokollen versteht man Protokolle, die unabhängig vom Anwendungsbereich sind [Alonso et al. 2004, S. 208].

Kontrolle als schwierig [Sit & Morris 2002]. Der schwerwiegendste Angriff, der als Sybil-Angriff bezeichnet wird, stellt dabei die Möglichkeit dar, dass ein Angreifer unter nahezu beliebig vielen Identitäten am P2P-System teilnehmen kann (vgl. [Douceur 2002]).

3.4.4 Einordnung von P2P-Systemen und -Netzen in den telekommunikationsrechtlichen Rahmen

Um das Potential aus betrieblicher Sicht einordnen zu können, müssen neben technischen Fragen auch ökonomische und juristische Aspekte Beachtung finden. Aus ökonomischer Sicht ist die Kosteneffizienz wie oben ausgeführt gegeben. Ferner existieren verschiedene Arbeiten wie zum Beispiel [Hausheer 2006], welche Abrechnungsmodelle und Preisbildung in P2P-Systemen fokussieren.

Aus juristischer Sicht bleibt jedoch offen, welche Rechte und Pflichten für den Betrieb von Peers gelten. Besonders erschwerend ist dabei die Tatsache, dass sich die rechtlichen Regelungen für verteilte Systeme und Rechnernetze deutlich unterscheiden. Dies wirft insofern die Frage auf, wie P2P-Systeme telekommunikationsrechtlich einzuordnen sind. Bislang liegt der Fokus der existierenden rechtlichen Arbeiten im Rahmen von P2P-Systemen jedoch ausnahmslos auf urheberrechtlichen Aspekten.

3.4.5 Konkretisierte Zielsetzung der Arbeit

Ziel der Arbeit ist es, das Potential von P2P-Systemen darzulegen. In Kapitel 2 wurden hierzu Grundlagen erläutert. In den weiteren Kapiteln werden folgende Aspekte vertieft diskutiert, die für den Betrieb und die Integration von P2P-Systemen in bestehenden Systemkontexten relevant sind:

- Integration von P2P-Techniken in bestehende Architekturen für verteilte Systeme
- Eignung von P2P-Techniken für Systeme mit wenigen Teilnehmern
- Robustheit von P2P-Systemen hinsichtlich Angriffen böswilliger Knoten
- Telekommunikationsrechtliche Verortung von P2P-Systemen und -Netzen

Die Darlegung von spezifischen verwandten Arbeiten wird in den jeweiligen Kapiteln vorgenommen.

3.5 Zusammenfassung

In diesem Kapitel wurde zunächst die Relevanz von P2P-Systemen im Internet und der Wissenschaft verdeutlicht. Dabei zeigte sich, dass P2P-Systeme in vielen Anwendungsbereichen Verwendung finden sowie skalierbar sind und selbst mit mehreren Millionen Teilnehmer funktionsfähig bleiben. Nach einer Identifikation von Kernelementen und wurde eine Einordnung und Bewertung der Technologie vorgenommen. Dabei zeigte sich, dass P2P-Systeme eine Virtualisierungseigenschaft aufweisen und durch Dezentralität geprägt sind. Weiterhin wurden die Eigenschaften von P2P-Systemen dargelegt.

Auf Basis dessen konnten schließlich Themenbereiche identifiziert werden, die einer vertieften Betrachtung bedürfen, um das Potential von P2P-Systemen aufzuzeigen. Diese offenen Fragen werden in den folgenden Kapiteln diskutiert.

4

Integrierte und kollaborative P2P-Architekturen

Bislang ist das Einsatzspektrum von P2P-Systemen vielfältig, jedoch auf abgegrenzte Anwendungsgebiete beschränkt. Im ersten Teil dieses Kapitels wird daher untersucht, inwieweit P2P-Techniken in bestehende Architekturen für verteilte Systeme integriert werden können. Hierzu wird eine dienstorientierte P2P-Architektur entwickelt, mittels derer sich auch komplexe verteilte Systeme wie eine elektronische Handelsplattform als P2P-System verwirklichen lassen.

P2P-Systeme selbst können vollständig dezentral und selbstskalierend realisiert werden. Für den Beitritt wird aber meist ein zentraler Bootstrap-Server genutzt. Da bei Mikro-P2P-Systemen mit wenigen Teilnehmern weniger die Skalierbarkeit, sondern vielmehr die Verfügbarkeit und somit die Dezentralität von Belang ist, stellt sich die Frage, ob Mikro-P2P-Systeme ohne Bootstrap-Server realisiert werden können. Im zweiten Teil des Kapitels wird daher eine kollaborative P2P-Architektur ohne zentrale Elemente aufgezeigt, die ein weit verbreitetes P2P-System (mit-)nutzt, um einen "dezentralen Beitritt" zu ermöglichen. Anhand einer umfangreichen empirischen Studie wird in einem realweltlichen P2P-System, der BitTorrent-DHT, die Tragfähigkeit des Ansatzes demonstriert. Ferner wird ein wahrscheinlichkeitstheoretisches Modell vorgestellt, das zur Bewertung und Optimierung dient und ein entsprechendes Verfahren, das die Suche in zukünftigen wesentlich beschleunigt.

4.1 Dienstorientierte P2P-Architektur

Um die Eignung und Integrationsmöglichkeiten von P2P-Techniken für komplexe verteilte Systeme zu untersuchen, werden zunächst typische Architekturen für verteilte Systeme dargelegt. Dabei zeigt sich, dass vor allem im organisationsübergreifenden Umfeld dienstorientierte Architekturen auf Basis von Web Services zielführend sind. In der Folge wird daher eine dienstorientierte P2P-Architektur entwickelt, welche die Vorteile beider Ansätze verknüpft. Zur Illustration der Herausforderungen und des entwickelten Lösungsansatzes wird zunächst ein exemplarisches Anwendungsszenario eingeführt.

4.1.1 Anwendungsszenario: Dezentrale elektronische Marktplattform

Die effiziente Nutzung von Energieressourcen ist gerade vor dem Hintergrund des weltweiten Klimawandels bedeutend. Ziel des Projektes *Selbstorganisation und Spontaneität in liberalisierten und harmonisierten Märkten (SESAM)* [WWW Prj Sesam] war es daher, im Rahmen des Anwendungsszenarios "Virtuelle Kraftwerke" zu untersuchen, wie eine effiziente Stromerzeugung und -nutzung durch einen Verbund von kleinen dezentralen Energieerzeugungsanlagen realisiert werden kann. Dabei sind insbesondere die Flexibilität der kleinen Anlagen hinsichtlich kurzfristiger Laständerungen und die Nähe zu den Energieverbrauchern vorteilhaft. Zur Förderung des Wettbewerbs sollten weder die Energieerzeugungsanlagen selbst noch die elektronische Marktplattform, über welche der Strom gehandelt wird, einem oder wenigen Betreibern unterstehen.

Im Gegensatz zu klassischen elektronischen Handelsplattformen, welche auf Client/Server-Architekturen basieren, soll dabei der dezentrale Ansatz auch auf Ebene der Handelsplattform konsequent weiterverfolgt werden, so dass auch auf dieser Ebene monopolartige Stellungen vermieden werden können. Insofern war es das Ziel, ein entsprechendes Rahmenwerk[1] zu entwickeln, dass den folgenden Zielen gerecht wird:

- Die Plattform soll ohne zentrale Komponenten auskommen, so dass kein dedizierter Betreiber notwendig ist. Zudem sollte die Architektur plattformunabhängig gestaltet werden.
- Zur Reduktion der Komplexität des Entwicklungs- und Wartungsaufwands des Systems, sollten modulare Komponenten zum Einsatz kommen.

[1] Bei einem Rahmenwerk (engl. Framework) handelt es sich um eine Menge von Klassen bzw. Komponenten, welche als wiederverwendbarer Entwurf für eine bestimmte Art von Systemen dienen [Gamma et al. 2004, S. 37].

- Die Architektur sollte skalierbar hinsichtlich der Teilnehmerzahl sein.
- Die Architektur sollte robust gegenüber dem Ausfall einzelner Knoten, aber auch gezielten Angriffen sein.
- Aus betrieblicher Sicht sollte zudem die rechtliche Einordnung solcher Architekturen vorgenommen werden.

Unter den gegebenen Rahmenbedingungen erscheint die Kombination von existierenden P2P-Netzen mit den klassischen Architekturen verteilter Systeme ein vielversprechender Lösungsansatz zu sein.

Die Architektur sollte dabei jedoch nicht auf ein P2P-Netz beschränkt bleiben, sondern die Integration von unterschiedlichen P2P-Netzen erlauben, da sich diese maßgeblich in ihren Funktionen und Eigenschaften unterscheiden. So ist bspw. eine unscharfe Suche nicht in jedem P2P-Netz möglich (vgl. Abschnitt 2.4.5).

4.1.2 Hintergrund und verwandte Arbeiten

P2P-Systeme sind verteilte Systeme, die jedoch häufig eine monolithische Architektur aufweisen. Demgegenüber stehen verschiedene Architekturmuster für "klassische" verteilte Informationssysteme, die im Laufe der letzten Jahrzehnte ausgehend von monolithischen bis hin zu N-Tier oder dienstorientierten Architekturen entwickelt wurden. Es ist insofern zielführend, die Integrationsmöglichkeiten von P2P-Techniken in solche Architekturen zu überprüfen. Daher werden zunächst elementare Aspekte von verteilten Systemen und deren Architekturen aufgezeigt.

Verteilte Informationssysteme

Ein verteiltes System unterscheidet sich von einem Rechnernetz vor allem dadurch, dass es sich dem Nutzer in einer kohärenten Weise darstellt und somit vom darunter liegenden System und Netzwerk abstrahiert [Tanenbaum 2003, S. 2]. Ein verteiltes Informationssystem lässt sich in drei Schichten gliedern [Alonso et al. 2004, S. 4 f]:

- **Darstellung:** Aufgabe der Darstellungsschicht (engl. Presentation Layer) ist die Interaktion mit den Nutzern und somit die Informationen darzustellen und Eingaben entgegenzunehmen. Die Darstellungsschicht kann bspw. in Form einer graphischen Nutzerschnittstelle (engl. Graphical User Interface, GUI) realisiert werden.
- **Applikationslogik:** Durch ein verteiltes Informationssystem werden Daten in der Regel nicht nur gespeichert, sondern auch verarbeitet. So erfordert bspw. ein Bibliotheksausleihsystem neben einer Bücherdatenbank

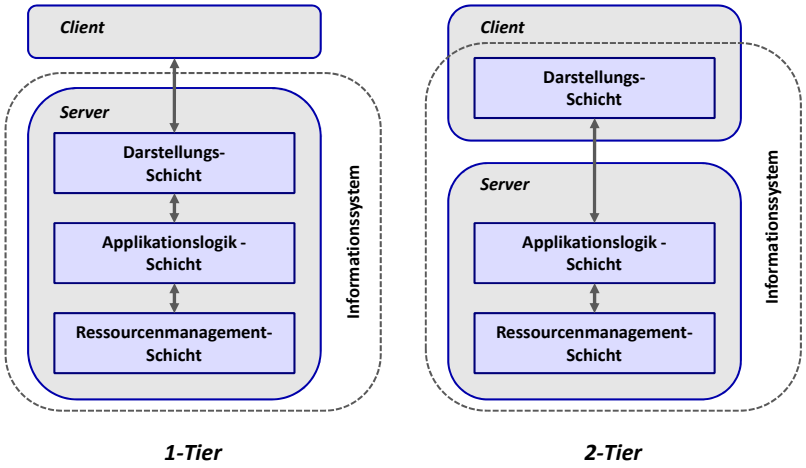


Abbildung 4.1: 1-Tier- und 2-Tier-Architekturen für verteilte Informationssysteme [Alonso et al. 2004]

verschiedene Funktionen, um eine Ausleihe von Büchern zu ermöglichen. Die Funktionen zur Datenverarbeitung werden in einer Applikationslogik-Schicht (engl. Application Logic Layer) gebündelt. Insofern finden sich in dieser Schicht die Geschäftsprozesse (engl. Business Process) wieder.

– **Ressourcenmanagement:** Die Speicherung von Daten, die Datenhaltung, findet in der Regel mittels Datenbanken oder in Dateisystemen statt. Die Schicht, in welcher die Datenhaltung erfolgt, wird daher als Ressourcenmanagement-Schicht (engl. Resource Management Layer) oder gelegentlich auch als Datenschicht (engl. Data Layer) bezeichnet[2]. In einer erweiterten Sicht kann es sich statt einer Datenbank auch um ein beliebiges externes System handeln, das Informationen bereitstellt. Insofern können mittels dieser Schicht andere Informationssysteme rekursiv integriert werden.

Bei verteilten Informationssystemen müssen all diese Schichten realisiert werden. Die möglichen Architekturformen unterscheiden sich aber hinsichtlich der Art und des Grades der Verteilung. In der Regel werden dabei die vier Architekturformen *1-Tier*, *2-Tier*, *3-Tier* und *N-Tier* unterschieden [Alonso et al. 2004, S. 9], die in Abb. 4.1 und 4.2 dargestellt sind.

Bei einer **1-Tier-Architektur** werden alle drei konzeptionellen Schichten eines Informationssystems auf einem Rechner implementiert. Insofern handelt es sich um ein monolithisches System. Aus historischer Sicht war eine solche Architektur oft die einzig mögliche und sinnvolle, da nur ein zentrales Mainframe-System

[2]Rechenressourcen werden implizit mit den Schichten assoziiert und nicht als eigene Schicht modelliert. Dies könnte sich jedoch vor dem Hintergrund der zunehmenden Verbreitung von Grids ändern (vgl. Abschnitt 2.3.3).

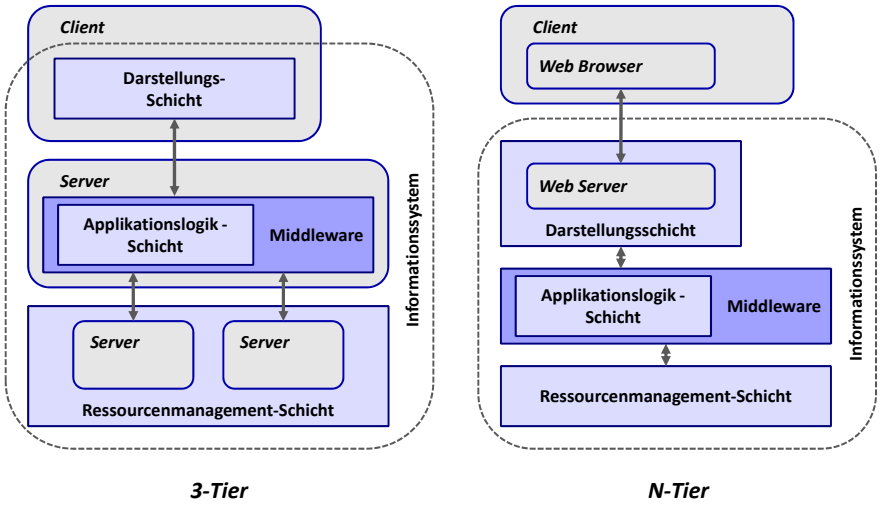


Abbildung 4.2: 3-Tier- und N-Tier-Architekturen für verteilte Informationssysteme [Alonso et al. 2004]

vorhanden war und die Darstellung mittels Terminals erfolgte, die keine Rechenkapazität besaßen. Dabei wurden in der Regel keine standardisierten bzw. stabilen Schnittstellen (engl. Application Programming Interface, API) vorgesehen. Vielmehr führten Leistungsoptimierungen dazu, dass die Grenzen verschwommen und die Schichten nicht klar getrennt waren.

Eine Aufteilung des Informationssystems in Client und Server wird durch die **2-Tier-Architektur** vorgenommen. Auf dem Server wird nach wie vor die Applikationslogik und die Datenhaltung realisiert. Die Darstellungsschicht wird auf den Client ausgelagert, so dass auf dem Server weniger Ressourcen benötigt werden. Diese Trennung erfordert eine klare Schnittstelle zwischen Applikationslogik- und Darstellungsschicht. Solch eine Architektur wurde mit dem Aufkommen von Personal Computern (PC) möglich und stellt insofern eine typische Client/Server-Architektur dar. Nachteilig wirkt sich bei einer 2-Tier-Architektur die immer noch limitierte Skalierbarkeit auf Seiten des Servers aus. Eine weitere Problematik entsteht, wenn ein Client mit mehreren Servern interagiert, da somit bei Änderungen der API eines Servers alle Clients geändert werden müssen.

Durch eine **3-Tier-Architektur** wird eine Trennung des Ressourcenmanagements und der Applikationslogik vorgenommen. Diese Trennung geht einher mit einer größeren Komplexität, eröffnet aber auch die Möglichkeit, auf Basis der so genannten Middleware-Schicht eine Integration unterschiedlicher Ressourcen durchzuführen. Außerdem können hierdurch auch andere Informationssysteme integriert werden, die dann der Middleware-Schicht als Ressourcen dienen. Durch diese Modularisierung kann die Last, wie in Abb. 4.2 dargestellt, auf mehrere Server verteilt werden, so dass sich die Skalierbarkeit der Architektur erhöht.

Eine **N-Tier-Architektur** ist eine verallgemeinerte 3-Tier-Architektur, die insbesondere das Internet als Zugangsmedium berücksichtigt. Abb. 4.2 zeigt beispielhaft eine N-Tier-Architektur, wobei eine 3-Tier-Architektur um einen Web-Server ergänzt wurde. Im Gegensatz zur 3-Tier-Architektur ist die Darstellungsschicht nicht auf den Client verlagert, sondern wird auf dem Web Server implementiert.

Synchrone vs. asynchrone Kommunikation: Die Kommunikation zwischen in einem verteilten Informationssystem erfolgt entweder *synchron* oder *asynchron*. Im Fall der synchronen Interaktion wartet der aufrufende Prozess bzw. Thread, bis eine Antwort von der entfernten Komponente eintrifft. Insofern wird auch von einem *blockierenden Aufruf* gesprochen. Erfolgt die Interaktion asynchron kann die Bearbeitung des Programms durch den entsprechenden Thread fortgesetzt werden, ohne dass auf eine Antwort gewartet werden muss. Man spricht daher auch von *nicht-blockierenden Aufrufen*. Bei der asynchronen Interaktion wird die Antwort von einem zweiten Thread entgegen genommen.

Die Realisierung einer asynchronen Interaktion ist im Allgemeinen zwar komplexer, erlaubt aber eine flexiblere Gestaltung der Systemkomponenten. So kann bspw. ein Publish/Subscribe-System realisiert werden, bei welchem die Adressierung von Nachrichten nicht direkt erfolgt, sondern mögliche Empfänger ihr Interesse an einer Nachricht einem vermittelnden System bekunden [Alonso et al. 2004, S. 22 ff]. Die Subskription erfolgt dabei anhand des Inhalts. Insofern spricht man auch in diesem Fall von inhaltsbasierter Adressierung (engl. Content-based Addressing) [Carzaniga & Wolf 2002].

Middleware: Die Middleware-Schicht in der 3-Tier- und N-Tier-Architektur dient zur Integration und nimmt insofern für verteilte Systeme eine zentrale Aufgabe wahr. Ziel der Middleware ist es, von den darunter liegenden Hard- und Software Komponenten wie Netzwerke, Betriebssysteme und Programmiersprachen zu abstrahieren [Coulouris et al. 2005, S. 16].

Eine Middleware besteht aus universellen Diensten, die für die Realisierung von verteilten Systemen hilfreich sind. In der Regel sind die Komponenten einer Middleware verteilt, laufen auf unterschiedlichen Plattformen und nutzen standardisierte Schnittstellen und Protokolle. Außerdem sind die Komponenten generisch und somit weder anwendungs- und domänenspezifisch [Bernstein 1996, S. 89 f].

Middleware Dienste bieten bspw. Funktionen zur Kommunikation, Verwaltung von Transaktionen und Verzeichnisse (vgl. [Bernstein 1996, S. 91]). Zur Kommunikation werden die Datenobjekte serialisiert und in ein plattformunab-

hängiges Format überführt. Sind mehrere Komponenten involviert, werden häufig Transaktionen genutzt, um die Daten konsistent zu halten bzw. bei Fehlern ausgeführte Aktionen rückgängig zu machen (engl. Rollback). Verzeichnisdienste werden bspw. benötigt, um Datenobjekte ausfindig zu machen, welche sich auf entfernten Rechner befinden.

Alle Middleware-Plattformen ermöglichen es, entfernte Methoden bzw. Objekte auf die gleiche Weise wie lokale aufzurufen. Diese Anbindung erfolgt durch so genannte *Client Stubs* und *Server Stubs* (vgl. u.a. [Alonso et al. 2004, S. 37 f]). Ein Client-Stub stellt dazu die Methoden des Servers als Rümpfe zur Verfügung. Wird eine solche Methode aufgerufen, wandelt der Client-Stub die übergebenen Parameter in ein Transportformat um (engl. *Marshaling*). Anschließend werden die Daten serialisiert und an den Server geschickt. Die notwendige Adresse des Servers wird in der Regel im Stub konfiguriert. Auf Seiten des Servers werden die empfangen Daten dem zuständigen Server-Stub zugewiesen und deserialisiert sowie in das passende Datenformat gewandelt (engl. *Unmarshaling*).

Als erste Form der Middleware gilt dabei der Aufruf von Methoden bzw. Prozeduren auf entfernten Rechnern, der als *Remote Procedure Call (RPC)* bezeichnet wird. Die RPC-basierten Middleware-Systeme ermöglichen es, die Aufrufe in einer einheitlichen und für die Anwendung transparenten Weise durchzuführen. Durch den Wechsel von der strukturierten hin zur Objekt-orientierten Programmierung entstand auch die Notwendigkeit mit entfernten Objekten zu interagieren. *Objekt-Vermittler (engl. Objekt Broker)* stellen daher die Weiterentwicklung des RPC-Paradigmas dar. Die verbreitetste Art von Objekt-Brokern basiert auf der *Common Object Request Broker Architecture (CORBA)*, welche von der Object Management Group spezifiziert wurde [WWW OMG]. Eine chronologische und prägnante Darstellung von Middleware-Systemen sowie Bewertung findet sich in [Alonso et al. 2004, S. 33 ff].

Dienstorientierte Architektur und Web Services

Die Möglichkeit schnell und flexibel auf Veränderungen der Märkte reagieren zu können, ist für moderne Unternehmen essentiell. Um dies durch IT-Systeme zu unterstützen, ist eine weitgehende Integration der Informationssysteme sowohl innerhalb eines Unternehmens als auch unternehmensübergreifend nötig.

Middleware-Systeme ermöglichen den Aufbau von modularen verteilten Systemen, die teilweise sehr komplex sind. Es war jedoch nicht das vorrangige Ziel der Middleware, bestehende Systeme zu integrieren oder Systeme über Unternehmens- bzw. Organisationsgrenzen hinweg zu verbinden. Um die Defizite existierender Middleware-Technologien zu überwinden, sind daher übergeordnete Architekturen und Technologien notwendig. In den letzten Jahren erlangte hierzu

vor allem das Konzept der *dienstorientierten Architektur (engl. Service-oriented Architecture, SOA)* in Verbindung mit der *Web Services*-Technologie erhebliche Bedeutung. Eine dienstorientierte Architektur ist zwar unabhängig von möglichen Technologien, die zur Realisierung eingesetzt werden. Insofern stellen Web Services nur eine mögliche Technologie dar. Gleichwohl nehmen Web Services eine dominierende Rolle ein (vgl. u.a. [Papazoglou & Heuvel 2007, S. 390]).

Dienstorientierte Architekturen in Verbindung Web Services stellen dabei eine Weiterentwicklung bzw. Ergänzung der bestehenden Middleware-Technologien hin zu unternehmensübergreifenden verteilten Systemen dar. So ist die einfachste Form einer Web Service-Kommunikation nichts anders als ein XML-basierter RPC. Aus diesem Beispiel wird bereits deutlich, dass der Standardisierung in diesem Bereich eine wesentliche Rolle zu kommt, um unternehmens-, aber auch plattformübergreifende Systeme zu ermöglichen. Die Komplexität solcher übergreifenden Systemen wird im Vergleich zu verteilten Systemen innerhalb einer Organisation zunehmen. Insofern kommt der Modularisierung in Form von Diensten neben der Standardisierung von Schnittstellen und Kommunikationsprotokollen bei dienstorientierten Architekturen eine wesentliche Rolle zu.

Alle Funktionen in einer SOA werden in Form von Diensten als wiederverwendbare Komponenten eines Geschäftsprozess zur Verfügung gestellt. Dabei ist es das Ziel, einer SOA komplexe Applikationen bzw. Systeme in Form von Diensten zu modularisieren. Die Dienste sollten dabei plattformunabhängig sein und dynamisch miteinander verknüpft werden können [Papazoglou & Heuvel 2007, S. 390].

Im Allgemeinen stellen Dienste eine abgeschlossene Einheit dar und sind autonom von anderen Diensten. Dienste zeichnen sich dabei durch eine klar definierte, stabile Schnittstelle aus, über welche sie genutzt werden können und die öffentlich bekannt ist [Alonso et al. 2004, S. 131].

Der Erfolg von Web-Technologien in den 1990er Jahren und die Schwierigkeiten bei der Kopplung unterschiedlicher Middleware-Plattformen führten dazu, dass auch eine plattformunabhängige Maschine-zu-Maschine-Kommunikation ermöglicht werden sollte. Nach der Definition des W3C handelt es sich bei einem Web Service um ein Software-System, welches eine Maschine-zu-Maschine Kommunikation über ein Netzwerk ermöglicht. Die Dienstschnittstelle wird dabei durch WSDL beschrieben und die Kommunikation findet mittels SOAP-Nachrichten statt, die über HTTP versandt werden. Insofern ist ein Web Service ein Dienst im Sinne einer dienstorientierten Architektur. Neben dieser gibt es noch weitere Definitionen, wobei die Kernelemente der genannten Definition allgemein anerkannt sind, da das W3C eine dominierende Stellung bei Web-Standards einnimmt [Alonso et al. 2004, S. 124].

> *"A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards."*
> gemäß W3C in [W3C wsa].

Für die Kommunikation mit Web Services wird meist das *SOAP*[3]-Protokoll [W3C Soap] genutzt. SOAP ist ein zustandsloses Protokoll, um XML-codierte Nachrichten auszutauschen. SOAP definiert hierzu einen generischen Rahmen, der durch weitere Spezifikationen erweitert werden kann. So ergänzt WS-Security [Oasis WSS] SOAP um sicherheitsspezifische Attribute und Mechanismen. Ferner werden vom W3C so genannte SOAP-Bindings definiert, die beschreiben, wie SOAP-Nachrichten mittels eines unterliegenden Protokolls wie HTTP zwischen zwei Knoten transferiert werden.

Um einen Dienst nutzen zu können, muss ein Dienstnehmer dessen Schnittstelle kennen. Bei Web Services erfolgt die Beschreibung der Dienstschnittstelle in der Regel mittels *WSDL (Web Services Description Language)* [W3C Wsdl]. Durch WSDL können die offerierten Methoden einschließlich den notwendigen Parametern und das entsprechende Antwortformat mittels eines XML-Formates spezifiziert werden.

Ferner stellt das Auffinden von Web Services einen elementaren Teil der Referenzarchitektur des W3C dar [W3C wsa]. Von einem Firmenkonsortium wurde hierzu *UDDI (Universal Description, Discovery, and Integration)* spezifiziert, welches mittlerweile von der OASIS als Standard gepflegt wird [Oasis UDDI]. Dienstverzeichnisse können zwei Funktionen erfüllen. Zum einen kann zur Entwicklungszeit ein passender Dienst gesucht werden. Zum anderen kann zur Laufzeit ein passender Dienst ausgewählt werden. Dabei spricht man auch von dynamischer Dienstbindung. Das ursprüngliche Ziel von UDDI war es, universelle öffentliche Verzeichnisse für komplett automatisierte elektronische Geschäftsprozesse bereitzustellen. Inzwischen wurde jedoch von diesen hoch gesteckten Zielen Abstand genommen. Der Fokus von UDDI liegt nun vielmehr auf dem Aufbau von unternehmensinternen Dienstverzeichnissen [Alonso et al. 2004, S. 296].

Abb. 4.3 zeigt das Zusammenspiel von Dienstgeber, -nehmer und -verzeichnis in einer *Web Services*-Architektur. Dabei wird nochmals deutlich, dass ein Dienstgeber seinen Dienst an einem zentralen Verzeichnis registriert. Ein Dienstneh-

[3] Ursprünglich war SOAP die Abkürzung für *Simple Object Access Protocol*. Da sich der Fokus des Protokolls mittlerweile jedoch geändert hat, soll nur noch die Abkürzung verwendet werden, um keine falschen Assoziationen zu wecken [W3C Soap 1.2].

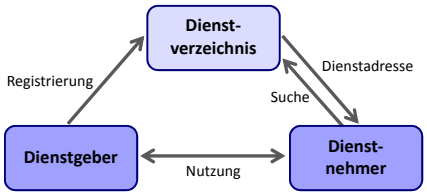


Abbildung 4.3: Zusammenspiel von Dienstgeber, -nehmer und -verzeichnis in einer *Web Services*-Architektur

mer kann anschließend den registrierten Dienst über das Verzeichnis finden. Die letztliche Dienstnutzung erfolgt direkt, d.h. Peer-to-Peer, zwischen dem Dienstnehmer und -geber.

Die Abgeschlossenheit der Dienste in Verbindung mit dem Konzept des dynamischen Bindens von Diensten führt vor allem bei dienstorientierten Architekturen auf Basis von Web Services dazu, dass vielfach von *lose-gekoppelten* Diensten gesprochen wird (vgl. u.a. [Alonso et al. 2004, S. 131]).

Eine ausgezeichnete Zusammenfassung zu den Themen verteilte Informationssysteme und Web Services findet sich in [Alonso et al. 2004]. Weitere Ausführungen zu dienstorientierten Architekturen finden sich unter anderem in [Papazoglou & Heuvel 2007] und [SOA Oasis], wo eine Referenzarchitektur spezifiziert wird.

P2P-Systemarchitekturen

P2P-Systeme sind in der Regel als monolithische Architekturen realisiert (vgl. [Androutsellis-Theotokis & Spinellis 2004, S. 338]). Darüber hinaus existieren jedoch auch verschiedene Ansätze die Funktionen von P2P-Systemen zu modularisieren, die im Folgenden vorgestellt werden.

Monolithische Systeme: Ein erstes Beispiel für ein monolithisches P2P-System ist Napster. Das System und Protokoll war speziell auf den Tausch von Musikdateien zugeschnitten und bestand aus einer Anwendung für die Peers sowie einem Index-Server (vgl. Abschnitt 2.2.1). Beide wurden von der Firma Napster entwickelt und es war weder eine Ergänzung der bestehenden Peer-Anwendungen noch eine Entwicklung unabhängiger Peer-Anwendungen vorgesehen. Die Schnittstelle des Index-Server war daher auch nicht als stabil zu betrachten, sondern konnte sich jederzeit ändern.

Gnutella wurde zunächst auch in Form einer proprietären Anwendungen entwickelt. Im weiteren Verlauf wurde das Protokoll öffentlich bekannt, so dass weitere unabhängige Implementierungen entstanden. Funktional ist das System auf

Dateitausch beschränkt und die Realisierung erfolgt nach wie vor als monolithische Anwendung. Auch andere P2P-Systeme sind ausschließlich für einen dedizierten Anwendungsbereich ausgelegt und als monolithische Anwendung realisiert. Wie bei klassischen verteilten Systemen können ohne Spezifikation und Stabilität der APIs nur monolithische Systeme realisiert werden.

Anwendungsschnittstellen von P2P-Systemen: Bei einigen neueren P2P-Systemen wie BitTorrent hat sich die Situation durch die Spezifikation der eingesetzten Protokolle etwas geändert (vgl. [WWW BitT Dev]), da die Schnittstellen und Protokolle als stabil anzusehen sind. Dennoch sind die Protokolle nur an einem einzelnen Anwendungsbereich ausgerichtet, so dass nach wie vor keine horizontalen anwendungsunabhängigen Protokolle spezifiziert wurden.

Ein weiteres Beispiel ist Skype das im Wesentlichen zur Sprachtelefonie und textbasierten Kommunikation genutzt wird (vgl. Abschnitt 2.4.4). Skype stellt eine API [WWW Skype API] bereit, um eigene Anwendungen zu entwickeln. Über diese Schnittstelle kann ein Zugriff auf die Funktionen der Skype-Anwendung erfolgen. Somit ist sowohl ein Zugriff auf höherwertige Funktionen wie zum Beispiel zur Etablierung einer Sprachverbindung möglich als auch der Aufbau von direkten Verbindungen zwischen zwei Skype-Clients, d.h. der Zugriff auf die Verzeichnisfunktion. Dennoch kann der Entwickler keinen Einfluss auf das eigentliche P2P-Netz nehmen, da das Kommunikationsprotokoll proprietär und darüber hinaus verschlüsselt ist (vgl. [Baset & Schulzrinne 2006]).

Verzeichnis-basierte Schnittstellen: Die meisten P2P-Systeme realisieren Verzeichnisse. So zum Beispiel Skype, um für einem Skype-Namen die aktuelle IP-Adresse nebst Port zu ermitteln, oder BitTorrent zur Realisierung des Trackerless-Modus. Skype bietet jedoch nur einen Zugriff auf dieses mittels der Skype-API und BitTorrent erlaubt ausschließlich die Speicherung der eigenen Netzwerkadresse (vgl. Abschnitt 2.4.4).

In [Dabek et al. 2003] wird eine gemeinsame API für strukturierte P2P-Netze beschrieben. Die API gliedert sich in drei Teile. Bei der untersten Ebene handelt es sich um die so genannten *Key-based Routing (KBR)*-Ebene. Auf der darüberliegenden Ebene, die in die drei Bereiche DHT, CAST (Anycast und Multicast) und DOLR (Decentralized Object Location und Routing) unterteilt ist, erfolgt eine Spezialisierung. Auf der dritten Ebene sind letztlich die konkreten Anwendungen angesiedelt. Die vorgesehene Schnittstelle der KBR-Ebene (KBR-API) ist für alle strukturierten P2P-Netze einheitlich und beinhaltet die drei Operationen:

- `route(Key k, Msg m, Node hint)`: Die Operation `route` dient dazu eine Nachricht `m` an das zuständige Peer weiterzuleiten. Das zuständi-

ge Peer wird durch den Parameter `k` bestimmt. Durch den optionalen Parameter `hint` kann ein Peer angegeben werden, das als nächstes benutzt werden soll.

- `forward(Key k, Msg m, Node nextHopNode)` : Mittels dieser Operation wird ein Aufruf der höherliegenden Ebene realisiert, einen so genannter Upcall, durch welchen der höheren Schicht die Weiterleitung einer Nachricht signalisiert wird. Die höhere Ebene kann dabei durch Setzen des `nextHopNode`-Parameters Einfluss auf die Weiterleitung der Nachricht nehmen. Diese Operation wird bei Knoten auf dem Pfad zum letztlich zuständigen Knoten aufgerufen.
- `deliver(Key k, Msg m)`: Die Operation `deliver` dient dazu die Nachricht beim zuständigen Knoten der höherliegenden Ebene weiterzureichen.

Weiterhin sieht die Arbeit eine DHT-API vor, welche aus den drei Operationen `put(key, data)`, `get(key)` sowie `remove(key)` besteht.

Für strukturierte P2P-Netze ist die präsentierte Schnittstelle nützlich, da sich insbesondere alle wesentlichen DHTs damit realisieren. Nachteilig bei der Arbeit [Dabek et al. 2003] ist, dass unstrukturierte P2P-Netze keine Berücksichtigung finden. Unstrukturierte Netze sind jedoch für unscharfe Suchanfragen besser geeignet (vgl. Abschnitt 2.4.2).

Ein generalisiertes Verzeichnis stellt OpenDHT [WWW OpenDHT] dar. Es handelt sich dabei um eine öffentliche DHT. In [Rhea et al. 2005b] wird sowohl die Funktion der DHT beschrieben, als auch die Tauglichkeit für verschiedene Anwendungen wie Namensauflösung oder als dezentraler Speicher aufgezeigt. Die DHT lässt die Speicherung von 20 Byte langen Schlüsseln in Verbindung mit maximal 1024 Byte großen Werten zu. Um die zur Verfügung stehenden Ressourcen fair zu verteilen, ist die Speicherdauer von Einträgen sowie der Platz pro Nutzer begrenzt. Betrieben wird OpenDHT als wissenschaftliches Projekt auf den Knoten des PlanetLab. Der Zugriff auf die DHT kann per XML-RPC erfolgen, wobei die Operationen `put`, `get` und `remove` zur Verfügung stehen.

Referenzarchitekturen und Plattformen: Ziel der Referenzarchitektur, die in [Aberer et al. 2005] präsentiert wird, ist es, einen generischen Rahmen für die Realisierung von P2P-Netzen zu spezifizieren. Die Architektur gliedert sich in eine P2P-Basisschicht und eine darüberliegende P2P-Speicherschicht. Die Basisschicht stellt grundlegende Funktionen zur Weiterleitung von Nachrichten bereit und ist insofern ähnlich zur KBR-API. Im Gegensatz zur KBR-API ist die Referenzarchitektur aber nicht auf strukturierte P2P-Netze beschränkt. Die Speicherebene stellt die Funktionen `insert`, `update`, `search` und `delete` zur

Verfügung, um Daten zu speichern. Ferner wird ein erweiterbares Klassendiagramm spezifiziert, welches als Basis für die Umsetzung von P2P-Netzen dient. Der Fokus der Arbeit liegt darauf, die elementaren Bestandteile von P2P-Netzen zu identifizieren. Insofern ist die Referenzarchitektur als Rahmen für P2P-Netze geeignet, bietet jedoch kaum Unterstützung hinsichtlich der Realisierung von P2P-Anwendungen bzw. -Diensten.

Neben spezifischen P2P-Systemen existieren zwei Plattformen, die zur Entwicklung von P2P-Systemen dienen. Dies ist zum einen die JXTA-Plattform von Sun Microsystems [Gong 2001]. Zum anderen bietet Microsoft basierend auf der .Net-Architektur ein Rahmenwerk für die Entwicklung von P2P-Anwendungen [WWW MS p2p 2008]. Beide Plattformen sind Rahmenwerke für die Entwicklung von P2P-Applikationen und stellen hierfür entsprechende Grundfunktionen bereit. JXTA nutzt dabei eine Superpeer-Architektur (vgl. Abschnitt 2.4.2), wobei die Superpeers in einer DHT organisiert sind [Traversat et al. 2003]. Wesentliches Element der Microsoft-Plattform ist das so genannte Peer-to-Peer Name Resolution Protocol (PNRP) [MS Pnrp 2006], das eine dezentrale Namensauflösung durch eine DHT ermöglicht.

Beide Plattformen sind jeweils auf einem P2P-Netz aufgebaut. Ferner ist die genaue Funktionsweise der eingesetzten P2P-Netz nicht veröffentlicht. Insofern eigenen sich die Plattformen nicht als Basis für eine dienstorientierte Architektur, da zwar gegebenenfalls Teile genutzt werden können, aber das parallele Anbieten mehrerer P2P-Netze nicht möglich ist.

Dienstorientierung bei P2P-Systemen: Ein nahe liegender Lösungsansatz um P2P-Techniken in dienstorientierten Architekturen zu integrieren, besteht darin das Dienstverzeichnis durch ein P2P-System zu realisieren (vgl. u.a. [W3C wsa, Abschn. 3.4.2.3] oder [Alonso et al. 2004, S. 139]. Solche Ansätze wurden bspw. in [Hoschek 2002], [Forster & De Meer 2004], [Vu et al. 2006] und [Sahin et al. 2005] aufgegriffen. In den Arbeiten entwickeln die Autoren unterschiedliche Konzepte, wie Dienste, in der Regel Web Services, beschrieben und diese Beschreibung durch ein P2P-System zugänglich gemacht werden können. Bei all diesen Ansätzen wird ein Dienst aber nach wie vor von einem Peer erbracht. Weiterhin wird in [Galatopoullos et al. 2008] beschrieben, wie eine Komposition von Diensten durch P2P-Techniken unterstützt werden kann. Die Arbeit baut auf JXTA auf und fokussiert vor allem die Dienstschicht. Auch in diesem Fall sind sowohl keine Dienst-spezifischen P2P-Netze als auch die Erbringung von Diensten durch mehrere Peers nicht möglich.

Darüber hinaus wird in [Gerke & Stiller 2005] und [Gerke & Hausheer 2005] ein dienstorientiertes Marktmodell beschrieben, bei welchem Dienste zu höher-

wertigen Diensten kombiniert werden können. Bei der entwickelten Architektur stehen jedoch weniger technische Aspekte im Vordergrund, so dass ein Dienst in dieser Architektur auch nur von einem Peer erbracht wird. Vielmehr fokussieren die Autoren auf Marktmodelle, Auktionen und Anreizsysteme.

Bewertung

Bevor eine zusammenfassende Bewertung stattfindet, werden zunächst nochmals die Anforderungen präsentiert, die sich aus dem Anwendungsszenario SESAM (vgl. Abschnitt 4.1.1) ergeben:

- **Modularisierung und horizontale Integration:** Aufgrund der Komplexität des Anwendungsszenario elektronischer Marktplatz sollte die Systemarchitektur eine Modularisierung zu lassen. Durch eine Modularisierung wird insbesondere der Entwicklungs- und Wartungsaufwand reduziert.

  Unter horizontalen Protokollen versteht man Protokolle, die unabhängig vom Anwendungsbereich sind [Alonso et al. 2004, S. 208]. Die Architektur sollte unterstützende, vom Anwendungsbereich unabhängige Dienste anbieten, so dass die Modulentwicklung unterstützt wird. Insgesamt kann somit auch ein hoher Grad der Wiederverwendbarkeit erreicht werden.
- **Dezentralität und Skalierbarkeit:** Eine Zentralisierung ist konträr zu typischen Geschäftsbeziehungen und soll daher vermieden werden (vgl. [Alonso et al. 2004, S. 130]). Um Single-Point-of-Failures aber auch eine zentralisierte organisatorische Kontrolle des Systems zu vermeiden, sollte dieses möglichst dezentral realisiert werden. Die Dezentralität sollte auch als Grundlage dienen, um das System skalierbar zu gestalten.
- **Selbstorganisation und Adaptivität**: Weiterhin sollte das System selbstorganisierend sein, um adaptiv und automatisiert veränderte Umgebungsbedingungen wie veränderte Lastsituationen oder Knotenausfällen reagieren zu können.
- **Organisationsübergreifend und plattformunabhängig:** Das System soll von vielen unterschiedlichen Marktteilnehmern eingesetzt werden, daher sollte es sowohl organisationsübergreifend als auch plattformunabhängig sein.

Vor dem Hintergrund der Anforderungen des Anwendungsszenarios sowie dem Überblick an Architekturmustern für verteilte Systeme erscheinen dienstorientierte Architekturen in Verbindung mit P2P-Techniken für den genannten Einsatzzweck zielführend.

	P2P-Systeme	SOA & Web Services
Modularisierung und horizontale Integration	–	+
Dezentralität und Skalierbarkeit	+	o
Selbstorganisation und Adaptivität	+	–
Organisations- und plattformübergreifend	o	+

Tabelle 4.1: Eignung von P2P-Systemen und dienstorientierten Architekturen & Web Services vor dem Hintergrund der Anforderungen des Anwendungsszenarios SESAM

Der Vorteil einer dienstorientierten Architektur besteht vor allem darin, dass eine sehr gute Modularisierung durch die Dienste möglich ist. Mittels der Standardisierungen bei Web Services und der entsprechenden Plattformen ist eine solide Grundlage hinsichtlich horizontaler Protokolle und anwendungsunabhängigen Funktionen geschaffen. Weiterhin wurden dienstorientierte Architekturen auf Basis von Web Services in Hinblick auf einen organisationsübergreifenden und plattformunabhängigen Einsatz gestaltet.

Die Kommunikation zwischen Dienstgeber und -nehmer erfolgt bereits direkt, also Peer-to-Peer. Zusätzlich ist bei dienstorientierten Architekturen jedoch ein zentrales Verzeichnis, so dass sich Dienstgeber und -nehmer finden. Kommt kein zentrales Verzeichnis zum Einsatz, müssen die Dienste, insbesondere deren Adressen, manuell konfiguriert werden, was letztlich weder adaptiv ist noch mit vielen Teilnehmern skaliert. Ferner sollte das System auch ohne zentrale Komponenten adaptiv auf ein geändertes Umfeld reagieren können. Um eine Zentralisierung bei den Dienstgebern selbst zu vermeiden und diesen adaptiv gegenüber Knotenausfällen gestalten zu können, sollte ein Dienst auch von mehreren Knoten realisierbar sein, wobei deren Koordination dann selbstorganisierend stattfindet.

P2P-Systeme können wie in Abschnitt 3.3.2 dargelegt, dezentral realisiert werden. Auch die Skalierbarkeit solcher Systemen konnte anhand von millionenfach genutzten Systemen nachvollzogen werden.

P2P-Systeme sind meist sehr gut vertikal integriert [Androutsellis-Theotokis & Spinellis 2004, S. 338], d.h. für einen dedizierten Anwendungsbereich gut geeignet sind. Bislang fand allerdings keine Standardisierung oder Spezifikation von allgemeinen Schnittstellen statt, wie es für eine horizontale Integration nötig wäre. Lediglich in Teilbereichen sind solche Aktivitäten zu erkennen. So ist bei bekann-

ten Architekturen auch nur ein P2P-Netz vorgesehen, das für den Einsatzzweck am besten geeignet ist. Im Sinne einer horizontalen Integration sollten in einem Rahmenwerk jedoch verschiedene P2P-Netze parallel genutzt werden können, da die Anforderungen der Anwendungsdienste unterschiedlich sein können und die P2P-Netze unterschiedliche Eigenschaften aufweisen (vgl. auch Abschnitt 2.4.5).

P2P-Systeme können zwar problemlos organisationsübergreifend eingesetzt werden. Die Plattformunabhängigkeit ist aber nicht in jedem Fall gegeben, da die Systeme meist monolithisch als einzelne Applikation realisiert sind und es somit davon abhängt ob die Applikation für die Zielplattform vorhanden ist.

Insofern sind die bislang entwickelten P2P-Architekturen und -Plattformen nicht ausreichend, da diese lediglich ein P2P-Netz vorsehen oder nur für bestimmte Arten von Netzen geeignet sind. Ein einfacher Lösungsansatz, der in bestehenden Arbeiten hinsichtlich Dienstorientierung und P2P-Netzen vorgeschlagen wurde, besteht darin, ein dezentrales Dienstverzeichnis zu etablieren. Nachteilig dabei ist, dass nur die Suche und nicht die Diensterbringung selbst durch mehrere Peers gemeinsam erfolgt und sie Skalierbarkeit fraglich bleibt.

In Tabelle 4.1 sind die dargelegten Gesichtspunkte in Verbindung mit den Anforderungen zusammengefasst.

4.1.3 Konzeption der dienstorientierten P2P-Architektur: Kollaborative Diensterbringung durch ServiceNets

In diesem Abschnitt werden die Grundkonzepte der entwickelten dienstorientierten P2P-Architektur erläutert. Hierzu wird zunächst die Grundidee formuliert. Anschließend werden exemplarische Dienste vorgestellt, die im weiteren Verlauf dieses und der folgenden Abschnitte zur Illustration dienen. Danach wird das Konzept der kollaborativen Diensterbringung durch so genannte ServiceNets erläutert.

> Die Grundidee besteht darin, eine dienstorientierte P2P-Architektur zu entwickeln, die P2P-Netze in den Rahmen einer dienstorientierten Architektur integriert. Dabei soll insbesondere die kollaborative Diensterbringung durch mehrere Peers und der parallele Einsatz von mehreren P2P-Netzen unterstützt werden.

Zur Umsetzung der dienstorientierten Architektur soll die Web Services-Technologie zum Einsatz kommen, da diese sowohl plattformunabhängig ist als auch für langlaufende Transaktion ausgelegt wurde, so dass die gegebenenfalls längeren Laufzeiten im P2P-Netz kein Problem darstellen.

Exemplarische Dienste

Um im Folgenden einzelne Aspekte illustrieren zu können, werden drei exemplarische Dienste eingeführt, welche für die Realisierung des eingeführten Anwendungsszenarios (vgl. Abschnitt 4.1.1) nötig sind.

- *Dokumentenverteildienst:* Dieser Dienst erlaubt, Dokumente wie zum Beispiel Stromangebote an die Teilnehmer zu verteilen, und bietet auch die Möglichkeit nach dem Dokument zu suchen. Dabei sollte eine unscharfe bzw. komplexe Suche möglich sein, d.h. die Suche sollte nicht auf einzelne Kennungen oder Schlüsselworte beschränkt sein und eine beliebige Zusammensetzung aus mehreren Suchbegriffen möglich sein.
- *Archivdienst:* Ziel eines Archivdienstes ist es, Dokumente wie Verträge zu archivieren, so dass sie beim Ausfall von Knoten dennoch verfügbar sind. Bedingt durch die reine Anforderung der Verfügbarkeit kann der Dienst auf komplexe Suchfunktionen verzichten und ausschließlich auf Dokumentenkennungen operieren. Die Dokumente können dabei verschlüsselt werden, um die Vertraulichkeit zu wahren.
- *Vertragsdienst:* Um basierend auf einem Stromangebot einen Vertrag zu schließen, müssen Nachrichten zwischen den beteiligten Vertragsparteien ausgetauscht werden. Der Austausch erfolgt dabei direkt, so dass lediglich ein Verzeichnisdienst nötig ist, welcher system- bzw. dokumentspezifische Kennungen in Netzwerkadressen auflöst.

ServiceNet

Die Diensterbringung durch mehrere Teilnehmer über die Grenzen einer Organisation hinweg zu unterstützten, ist ein zentrales Element der anvisierten dienstorientierten P2P-Architektur. Hierzu dient das entwickelte Konzept *ServiceNet*.

Ein ServiceNet besteht aus einer Menge von Knoten, die gemeinsam einen Dienst bereitstellen. Ein ServiceNet kann bspw. zur Verteilung von Dokumenten wie Stromangeboten dienen, d.h. einen Dokumentenverteildienst realisieren. Abb. 4.4 zeigt zwei exemplarische ServiceNets. Dabei ist ersichtlich, dass ein Knoten einerseits an mehreren ServiceNets teilnehmen kann und andererseits nicht alle Peers an jedem ServiceNet teilnehmen müssen. Die Nutzung eines ServiceNets kann sowohl durch teilnehmende Peers (intern) als auch nicht-teilnehmende Peers (extern) erfolgen. Eine externe Nutzung eines ServiceNets ist insbesondere bei Geräten mit wenigen Ressourcen wie zum Beispiel Mobilfunktelefonen sinnvoll. Als Ganzes stellt ein ServiceNet somit wieder einen Dienst dar, der über eine stabile Schnittstelle und verschiedene Zugangspunkte verfügt. Der Dienstzugriff ist dabei über jedes teilnehmende Peer möglich.

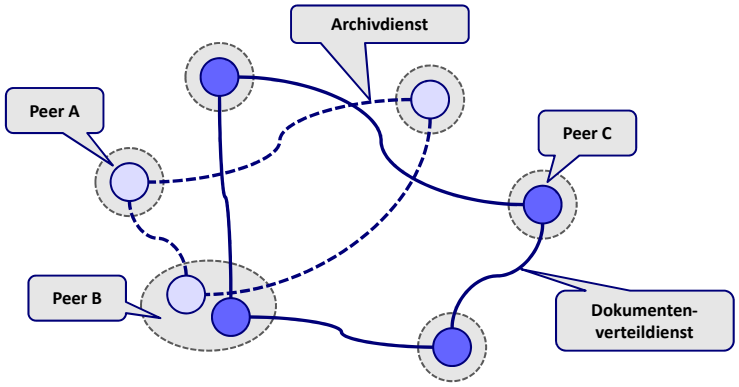


Abbildung 4.4: *ServiceNets* zur kollaborativen Diensterbringung

In funktionaler Hinsicht unterscheidet sich ein ServiceNet nicht von einem Dienst, der von einem einzelnen Teilnehmer erbracht wird. Es sind vielmehr die nicht-funktionale Eigenschaften wie Dienstgüte oder die Anzahl der zur Verfügung stehenden Ressourcen bzw. Inhalte, durch welche sich ein ServiceNet von einem herkömmlichen Dienst unterscheidet. Da ein ServiceNet auf P2P-Netzen beruht, können sich folgende nicht-funktionalen Eigenschaften auf das ServiceNet übertragen:

- Die Skalierbarkeit kann durch Hinzunahme neuer Peers sichergestellt werden. Dabei ist vor allem das Selbst-Management und die Selbst-Konfiguration von P2P-Netzen von Vorteil, um eine nahtlose Integration und Nutzung der Systemressourcen zu gewährleisten. Darüber hinaus werden Engpässe durch zentrale Komponenten vermieden.

- Ebenso wie P2P-Netze, können auch ServiceNets den Ausfall von Knoten kompensieren und der Dienst als Ganzes bleibt verfügbar.

- Durch die Kollaboration mehrerer Peers kann die Qualität bzw. der Wert eines ServiceNets insofern steigen, dass mehr Inhalte zur Verfügung stehen und nicht die Abfrage vieler einzelner Dienste notwendig ist.

Zur Kommunikation und Koordination der Teilnehmer nutzt jedes ServiceNet ein unterliegendes P2P-Netz. Da nicht jeder Dienst die gleichen Anforderungen an ein P2P-Netz hat, bedarf es der Unterstützung unterschiedlicher P2P-Netze. Die Auswahl des passenden P2P-Netzes erfolgt anhand der Dienstanforderungen. Ein Dokumentenverteildienst benötigt bspw. eine unscharfe Suche, die sich mit einer DHT nicht realisieren lässt, während ein Archivdienst gegebenenfalls ausschließlich auf eindeutigen Dokumentenkennungen operieren kann und sich somit mittels DHTs realisieren lässt. Für die Auswahl von geeigneten P2P-Net-

zen können Klassifikationen wie [Lua et al. 2005], [Mischke & Stiller 2004] oder [Risson & Moors 2006] genutzt werden (vgl. auch Abschnitt 2.4.5).

Für die Suche nach ServiceNets kann anstatt eines zentralen Dienstverzeichnisses ein Meta-ServiceNet verwendet werden, in welchem existierende ServiceNets verzeichnet sind.

Knotenarchitektur

Die Realisierung der ServiceNets erfordert eine Knotenarchitektur, welche sowohl unterschiedliche P2P-Netze integriert als auch einen Rahmen für Dienste bereitstellt. Um die Dienstentwickler zu entlasten, sollten P2P-Netze als Module zur Verfügung stehen und vom eigentlichen Dienst entkoppelt sein. Die Dienste selbst werden als Web Services realisiert, um den Anforderungen hinsichtlich Plattformunabhängigkeit sowie der organisationsübergreifenden Kommunikation gerecht zu werden. Die entwickelte Architektur, die in Abb. 4.5 dargestellt ist, gliedert sich in folgende Teile:

- **Kommunikationsschicht:** Die unterste Ebene, die so genannte Kommunikationsschicht, abstrahiert von Kommunikationsprotokollen wie TCP oder UDP. Insofern werden hierdurch auch alle tieferliegenden Protokolle, wie zum Beispiel IP oder Ethernet gekapselt. Aufgabe der Schicht ist es, durch Angabe einer entsprechenden Netzwerkadresse, wie IP-Adresse nebst Port, eine Verbindung zwischen zwei Peers aufbauen zu können.

- **Overlay-Schicht:** Die P2P-Schicht beinhaltet verschiedene P2P-Netze, wie zum Beispiel Chord oder Gnutella als Module. Die Module werden der darüberliegenden Schicht über eine universelle Schnittstelle zur Verfügung gestellt. Somit ist auch ein Austausch des P2P-Netzes durch Änderung der Konfiguration möglich, wobei die Verwaltung und Konfiguration der P2P-Module mittels des Dienst- und P2P-Managements erfolgt.

  Die P2P-Module beinhalten die jeweiligen P2P-Netz-spezifische Verfahren zum Routing von Datenpaketen, Aufbau und Pflege der Routing-Tabelle etc. Insofern können die P2P-Module auch entsprechend der Referenzarchitektur in [Aberer et al. 2005] realisiert werden.

- **Dienststeuerungsschicht:** Dienste greifen nicht direkt auf die P2P-Module zu, sondern mittels der Dienststeuerungsschicht, die im Wesentlichen einen so genannten SOAP-Prozessor beinhaltet. Der SOAP-Prozessor serialisiert und deserialisiert XML-codierte SOAP-Nachrichten in plattformspezifische Dienstaufrufe und ausgehende Nachrichten entsprechend um-

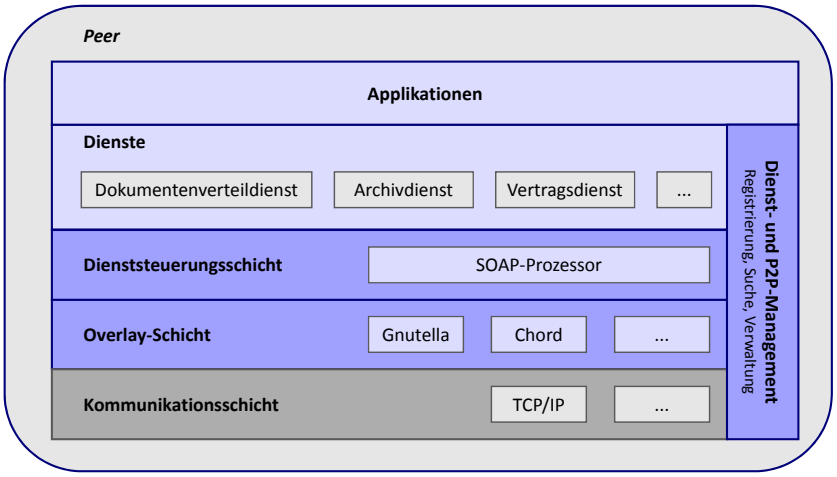


Abbildung 4.5: Dienstorientierte P2P-Architektur aus Sicht eines Knotens

gekehrt (vgl. "Marshaling" durch die Middleware in Abschnitt 4.1.2). Darüber hinaus wird von der Dienststeuerungsschicht sichergestellt, dass die SOAP-Nachrichten über das passende P2P-Netz versendet und beim Empfang dem korrekten Dienst zugeordnet werden. Hierzu wird auf die Konfigurationsdaten des Dienst- und P2P-Management-Teils zurückgegriffen.

- **Dienst- und P2P-Management:** Ein Kernelement der dienstorientierten P2P-Architektur stellt das Dienst- und P2P-Management dar. Durch dieses wird die Konfiguration der P2P-Module und Dienste sowie deren Zuordnung verwaltet. Somit wird hierdurch auch die Zugehörigkeit zu entsprechenden ServiceNets bestimmt. Ferner unterstützt das Dienst- und P2P-Management die Suche und Registrierung nach Diensten durch die Realisierung eines verteilten Dienstverzeichnisses.

- **Dienste & Applikationen:** Die Anbindung der Dienste erfolgt mittels der für Web Services typischen Stubs (vgl. Middleware in Abschnitt 4.1.2). Die Interaktion mit dem Nutzer erfolgt schließlich aufbauend auf den Diensten in der Applikationsebene. In der Abb. 4.5 sind die eingeführten exemplarischen Dienste des Anwendungsszenarios dargestellt.

Die Dienststeuerungsschicht stellt in Verbindung mit der Overlay-Schicht sowie dem Dienst- und P2P-Managements insofern typische Middleware-Funktionalitäten bereit.

Adressierung der Knoten in ServiceNets

Typischerweise erfolgt bei Web Services die Adressierung zwischen Dienstnehmer und Dienstgeber, indem die Adresse des Dienstgebers zuvor manuell konfiguriert oder dynamisch mittels eines Dienstverzeichnisses wie UDDI ermittelt wird. Beiden Adressierungsarten ist gemein, dass die Adressierung unabhängig vom Dienstaufruf, d.h. unabhängig von der resultierenden SOAP-Nachricht ist. Die Adressierung bei P2P-Systemen und somit auch ServiceNets erfolgt hingegen inhaltsbasiert, so dass eine feste Konfiguration, wie bei Web Services üblich, nicht möglich ist. Insofern ist eine dynamische, vom Dienstaufruf abhängige, Adressierung notwendig. Die entwickelte dienstorientierte P2P-Architektur sieht daher drei Möglichkeiten zur Adressierung vor.

Die Anbindung der Dienstnehmer und -geber erfolgt, wie bereits bei der Knotenarchitektur erläutert, mittels Stubs, d.h. die Aufrufe werden durch den SOAP-Prozessor der Dienststeuerungsschicht in entsprechende SOAP-Nachrichten umgewandelt. Wird eine SOAP-Nachricht empfangen, erfolgt durch den SOAP-Prozessor der Aufruf des entsprechenden Stubs. Anschließend wird die SOAP-Nachricht an das entsprechende P2P-Modul in der Overlay-Schicht weitergereicht. Um dem P2P-Modul das Versenden der SOAP-Nachricht zu ermöglichen, stehen drei Adressierungsmöglichkeiten zur Verfügung:

- **P2P-Netz-basierte Adressierung:** Diese Adressierungsart ist unabhängig von der SOAP-Nachricht selbst, d.h. das P2P-Netz-Modul kann selbstständig den passenden Knoten und dessen Adresse ermitteln. Wird bspw. für den Dokumentenverteildienst ein Gnutella-Netz genutzt, erfolgt die Verteilung der Dokumente rein auf Basis der Algorithmen des Gnutella-Netzes. Zusätzliche Informationen über die SOAP-Nachricht und Interaktionen mit den anderen Schichten der Knotenarchitektur sind in diesem Fall nicht nötig. Diese Adressierungsart ist der bei Web Services üblicherweise verwendeten Adressierung sehr ähnlich, da kein Bezug auf die SOAP-Nachricht erfolgt.
- **SOAP-Nachrichten-basierte Adressierung:** Nicht in jedem Fall ist es möglich, dass P2P-Module ohne weitere Informationen entscheiden können, an welchen Knoten eine SOAP-Nachricht versendet werden muss. Hängt der zuständige Knoten vom Nachrichteninhalt ab, kann dieser Knoten durch Analyse der SOAP-Nachricht bestimmt werden. Werden bspw. durch einen Archivdienst Dokumente gespeichert und es wird hierzu eine DHT genutzt, kann die Berechnung des entsprechenden Schlüssels anhand einer etwaigen Dokumentenkennung erfolgen, die in der SOAP-Nachricht enthalten ist.

  Die Analyse der SOAP-Nachricht und Extraktion des adressierungsrele-

vanten Elementes findet durch die Dienststeuerungsschicht statt. Das extrahierte Element wird anschließend dem P2P-Modul übergeben. Somit müssen die P2P-Module SOAP-Nachrichten nicht interpretieren können, sondern können diese als Black-Box betrachten. Im Dienst- und P2P-Management wird konfiguriert, anhand welches Elementes des SOAP-Nachricht der Schlüssel berechnet wird.

– **Nachrichtenkontext-basierte Adressierung:** Teilweise ist der Zugriff auf die für die Adressierung maßgeblichen Nachrichtenelemente nicht ohne Weiteres möglich, da die Daten nicht in der SOAP-Nachricht enthalten oder nur Teil komplexer Datenstrukturen der SOAP-Nachricht sind. In diesem Fall kann beim Dienstaufruf ein so genannter Nachrichtenkontext definiert werden, in welchem ein adressierungsrelevantes Element übergeben wird. Nachrichtenkontexte stellen dabei eine zusätzliche Datenstruktur dar, in welcher Meta-Informationen zu einem Dienstaufruf enthalten sind. Dadurch bleibt die eigentliche Dienstschnittstelle und resultierende SOAP-Nachricht unberührt. Die Nachrichtenkontexte sind dabei der Dienststeuerungsschicht zugänglich, die das adressierungsrelevante Element wiederum an das P2P-Modul weiterleitet.

4.1.4 Prototypische Implementierung

Zur Evaluierung der Konzepte wurde die konzipierte dienstorientierte P2P-Architektur im Rahmen einer prototypischen Implementierung realisiert. In diesem Abschnitt werden relevante Aspekte der Implementierung skizziert und die elementaren Teile des zugrunde liegenden UML-Klassendiagramms präsentiert.

Die Implementierung fand im Rahmen des vorgenannten SESAM-Projektes statt (vgl. Abschnitt 4.1.1). Als Plattform für die Implementierung wurde Java gewählt, da hierdurch auch die Applikationen und Dienstimplementierungen plattformunabhängig sind. Aufgrund der Web Services-basierten Architektur könnte jedoch problemlos bspw. ein .Net-basierter Prototyp implementiert werden.

Grundlage der Implementierung bildet die Web Service-Implementierung der Apache Software Foundation, die als *Apache Axis* bezeichnet wird [WWW Axis]. Für die Implementierung wurde *Apache Axis Version 1.2* verwendet, da dies zum Zeitpunkt der Erstellung des Prototypen, die am besten geeignetste Plattform für Web Services auf Basis der Java-Plattform darstellte.

Es wurden die beiden P2P-Module Gnutella und Chord implementiert. Ebenso eine Reihe von Diensten, die zur Umsetzung des Anwendungsszenarios elektronischer Marktplatz (vgl. Abschnitt 4.1.1) nötig waren. Darin waren auch die zuvor erwähnten drei exemplarischen Dienste enthalten.

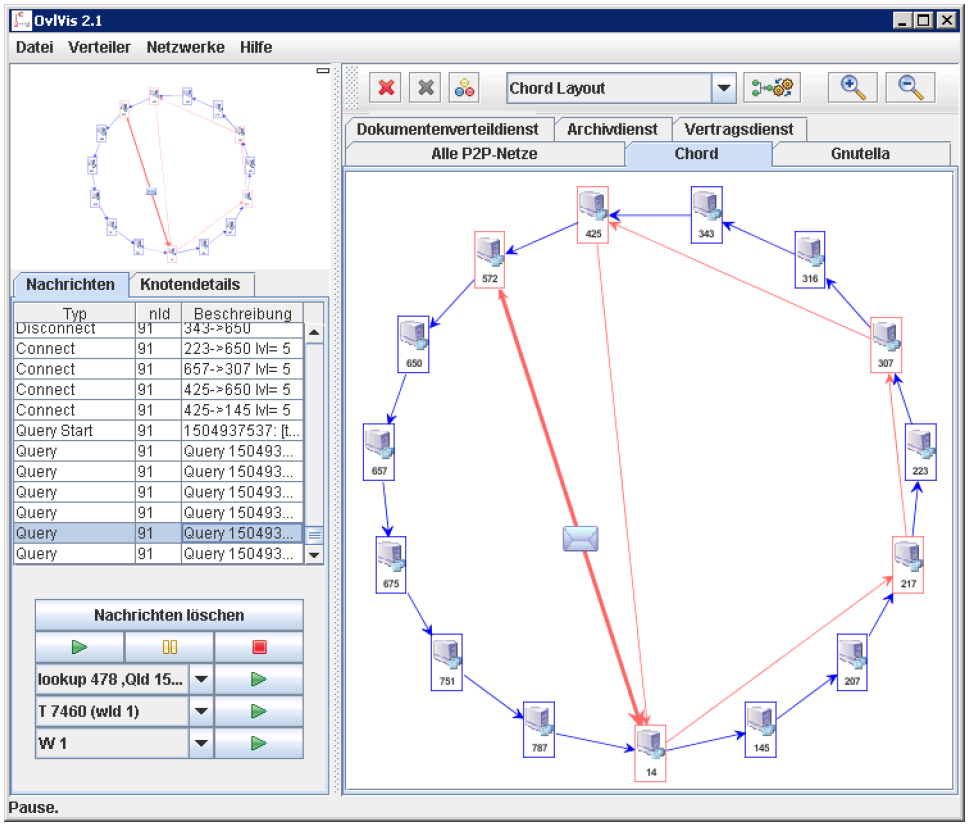


Abbildung 4.6: Screenshot des Overlay-Netzwerk-Visualisators *OvlVis*

- *Dokumentenverteildienst:* Der Dokumentenverteildienst erlaubt die Verteilung von und Suche nach Dokumenten wie zum Beispiel Stromangeboten. Der Dienst wurde mit dem P2P-Modul Gnutella kombiniert, so dass auch eine unscharfe Suche möglich ist. Als Adressierungsart kommt dabei die P2P-Netz-basierte Adressierung zum Einsatz.
- *Archivdienst:* Ziel eines Archivdienstes ist es, Dokumente wie Verträge zu archivieren. Der Dienst wurde in Kombination mit dem P2P-Modul Chord realisiert. Da in den ausgetauschten SOAP-Nachrichten eine Dokumentenkennung enthalten ist, wird die SOAP-Nachrichten-basierte Adressierung genutzt. Die Dokumente werden dabei als Wert eines Schlüssel/Wert-Paares gespeichert, wobei der Schlüssel der gehashten Dokumentenkennung entspricht.
- *Vertragsdienst:* Für den direkten Nachrichtenaustausch zwischen zwei Knoten beim Vertragsschluss, wurde der Vertragsdienst implementiert. Dieser bedient sich auch dem P2P-Modul Chord und nutzt dieses als eine Art Verzeichnisdienst. Die Adressierung kann somit unabhängig von IP-Adressen stattfinden und Probleme durch dynamische IP-Adressvergabe etc. kön-

nen umgangen werden. Da der Vertragspartner nicht in den ausgetauschten SOAP-Nachrichten enthalten ist, wird die Nachrichtenkontext-basierte Adressierung angewandt.

OvlVis – Visualisierung von Overlay Netzen: Mittels des Prototypen konnten die Tragfähigkeit der Konzepte erfolgreich nachvollzogen werden. Hierzu wurde insbesondere auch eine Anwendung zur Visualisierung der Overlay-Netze, die durch die P2P-Module aufgespannt werden, entwickelt. Diese Anwendung wird als *OvlVis* bezeichnet. *OvlVis* kann einerseits als Monitoring-Software genutzt werden, um die aktuellen Ereignis innerhalb eines oder mehrerer P2P-Netze zu verfolgen. Andererseits ermöglicht *OvlVis* vergangene Ereignisse in Form eines "Play-Backs" nachzuvollziehen. Abb. 4.6 zeigt einen exemplarischen Screenshot von *OvlVis*. Auf dem Screenshot ist zu sehen wie eine Nachricht durch ein Chord-Netz geroutet wird. Eine detaillierte Beschreibung der Applikation sowie deren modulare Architektur findet sich in [Jünemann & Dinger 2008].

UML-Klassendiagramm: Die Umsetzung der Architektur in Form eines UML-Klassendiagramms zeigt Abb. 4.7. Das Diagramm enthält, um die Übersichtlichkeit zu wahren, nur die elementaren Klassen und Methoden.

In dem Paket `overlay` sind die Basisklassen für die Overlay-Schicht enthalten. Die zentrale Klasse ist `OvlModule`, die zur Implementierung der P2P-Module dient. Die Klasse `OvlKey` entspricht einem Schlüssel wie er von den P2P-Modulen verwendet wird und `OvlMsg` einer Nachrichten, die zwischen Knoten ausgetauscht wird. Jedes P2P-Modul erbt von der Klasse `OvlModule` und ist wiederum assoziiert mit einem `OvlKeyModule`, einem `OvlHandler` und einem `OvlSrvHandler`. Die Methode `sendRcv` dient zum Senden und Empfangen von Datenpaketen. Durch die Methode `init` erfolgt die Initialisierung des `OvlModul`. Die Methoden `start` und `stop` dienen dazu dem entsprechenden P2P-Netz beizutreten bzw. auszutreten. Durch das P2P-Netz empfangene Nachrichten werden mittels der Schnittstelle `OvlHandler` weitergereicht.

Die Klasse `OvlKeyModule` dient dazu Schlüssel entsprechend des P2P-Netzes zu berechnen und zu bestimmen, ob ein Knoten für einen bestimmten Schlüssel zuständig ist (`isResponsible`). So wird bspw. bei der Implementierung des P2P-Moduls Chord durch die Methode `calcKey` die Zeichenkette `str` auf einen 160 bit Schlüssel abgebildet, der in `OvlKey` gekapselt wird. Um Diensten zu ermöglichen auf geänderte Zuständigkeiten im P2P-Netz zu reagieren, die zum Beispiel durch den Beitritt eines Knotens entstehen, kann der Dienst die Schnittstelle `OvlSrvHandler` implementieren.

Mittels des Pakets `serviceHandling` wird die Dienststeuerungsschicht

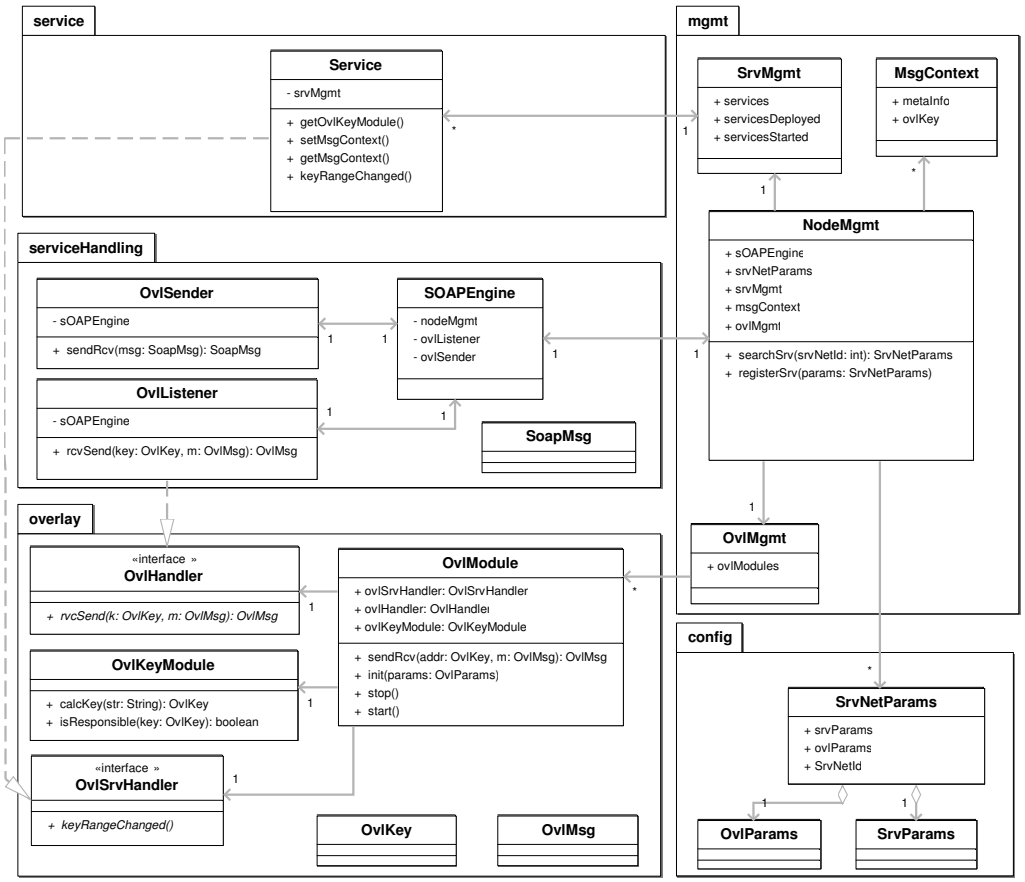


Abbildung 4.7: Umsetzung der dienstorientierten P2P-Architektur in Form eines UML-Klassendiagramms

realisiert. Die Klasse `SOAPEngine` dient im Wesentlichen als Abstraktion für den SOAP-Prozessor, welcher SOAP-Nachrichten in plattformspezifische Aufrufe umwandelt. Mit der `SOAPEngine` sind die beiden Klassen `OvlSender` und `OvlListener` assoziert, die zum Empfang und zum Senden von Nachrichten dienen und insofern die Verbindung zur Overlay-Schicht schaffen.

Im Paket `service` ist die Klasse `Service` enthalten, die als Basis für die Implementierung von Diensten dient. Ein Zugriff auf Nachrichtenkontexte ist dabei durch die Methoden `setMsgContext` und `getMsgContext` möglich. Die Implementierung der Schnittstelle `OvlSrvHandler` erfolgt durch die Methode `keyRangeChanged`. Die Methode `getOvlKeyModule` dient zur Berechnung von Schlüsseln wenn Nachrichtenkontexte zum Einsatz kommen.

Das Paket `mgmt` beinhaltet die elementaren Klassen, die zur Verwaltung der Dienste (`SrvMgmt`) und der P2P-Module (`OvlMgmt`) benötigt werden. Der Zugriff auf die Verwaltung erfolgt mittels der Klasse `NodeMgmt`, über welche auch eine Registrierung von und Suche nach Diensten möglich ist. Die Konfigurati-

on der ServiceNets erfolgt mittels der Klasse `SrvNetParams`, welche sich wiederum aus `OvlParams`, der P2P-Modul-Konfiguration, und `SrvParams`, der Dienstkonfiguration zusammensetzt.

4.1.5 Bewertung

Die Bewertung in diesem Abschnitt erfolgt ausgehend von den Anforderungen und Defiziten der bestehenden P2P-Systemarchitekturen respektive dienstorientierten Architekturen, wie sie in Abschnitt 4.1.2 dargelegt wurden. Eine zusammengefasste Darstellung erfolgt in Tabelle 4.2.

Modularisierung und horizontale Integration: P2P-Systeme weisen meist eine gute vertikale Integration auf, d.h. sie sind für einen Anwendungsbereich optimiert, generalisierte stabile Schnittstellen fehlen jedoch. Durch die dienstorientierte P2P-Architektur wird eine horizontale Integration von P2P-Netzen vorgenommen, so dass diese für einen breiten Anwendungsbereich zugänglich sind.

Im Unterschied zu anderen P2P-Systemarchitekturen ermöglicht die entwickelte *dienstorientierte P2P-Architektur* eine flexible und parallele Nutzung verschiedener P2P-Netze. Die P2P-Netze werden hierzu in so genannten *P2P-Modulen* gekapselt. Außerdem wurden die Dienste und P2P-Module entkoppelt. Die Bindung erfolgt ausschließlich durch entsprechende Konfiguration. Die Auswahl des passenden P2P-Netzes erfolgt aus Basis der jeweiligen Dienstanforderungen.

Darüber hinaus findet durch die Nutzung der Web Services-Technologie eine Modularisierung des Systems in Form von Diensten statt. Die Dienstorientierung erlaubt auch eine vereinfachte Integration in bestehende verteilte System.

Dezentralität und Skalierbarkeit: Dezentralität und Skalierbarkeit sind typische Eigenschaften von P2P-Systemen. Fraglich blieb jedoch wie klassische verteilte Systemarchitekturen dezentral realisiert werden können.

Bei klassischen 3-Tier- bzw. N-Tier-Architekturen erfolgt die Modularisierung anhand der Schichten wie sie in Abb. 4.2 dargestellt sind. Es erfolgt eine funktionale Aufteilung zu Rechnersystemen (Servern). Die Diensterbringung erfolgt durch einzelne Systeme.

Durch das entwickelte Konzept des *ServiceNet* wird in Ergänzung zu der funktionalen Aufteilung eine kollaborative Diensterbringung mittels mehrerer Knoten ermöglicht. Insofern werden somit auch die Dienste selbst dezentralisiert. Weiterhin wird die Skalierbarkeit des Systems durch das Konzept der ServiceNets und die kollaborative Diensterbringung gesteigert, da leicht neue Systemressourcen integriert werden können. Ferner können zentrale Verzeichnisdienste, wie sie in klassischen Middleware-Systemen und dienstorientierten Architekturen nötig

	P2P	SOA	**Dienst. P2P-Arch.**
Modularisierung und horizontale Integration	–	+	+
Dezentralität und Skalierbarkeit	+	o	+
Selbstorganisation und Adaptivität	+	–	+
Organisations- und plattformübergreifend	o	+	+

Tabelle 4.2: Dienstorientierte P2P-Architektur im Vergleich zu P2P-Systemen und dienstorientierten Architekturen & Web Services vor dem Hintergrund des Anwendungsszenarios SESAM (vgl. auch Tabelle 4.1)

sind, durch ein Zusammenwirken der Knoten vermieden werden. Hierzu wurde eine verteiltes Dienstverzeichnis realisiert.

Selbstorganisation und Adaptivität: Das Zusammenspiel der Ressourcen in herkömmlichen dienstorientierten Architekturen ist durch eine feste Konfigurationen geprägt. Bei *ServiceNets* ist hingegen durch die P2P-Netze eine dynamische und adaptive Ressourcennutzung und somit auch Selbstkonfiguration möglich. Insofern wird durch die dienstorientierte P2P-Architektur ein neuartiger Middleware-Dienst zur dynamischen Ressourcennutzung geschaffen.

Die Anbindung der Dienste erfolgt mittels Stubs. Da für ServiceNets eine feste Konfiguration der Rechneradressen nicht zielführend ist, wurden entsprechende Adressierungsverfahren entwickelt, die eine dynamische, *inhaltsbasierte Adressierung* erlauben. Die dargelegten Adressierungsarten zeichnen sich vor allem dadurch aus, dass die Definition der Dienstschnittstellen davon unberührt bleibt und dennoch eine inhaltsbasierte Adressierung ermöglicht wird.

Organisationsübergreifend und plattformunabhängig: Indem die standardisierte Web Services-Technologie genutzt wird, wird die Architektur soweit möglich den Anforderungen organisationsübergreifend und plattformunabhängig gerecht. Die Kommunikation zwischen den P2P-Modulen erfolgt jedoch nach wie vor direkt ohne standardisierte Protokolle. Dies wäre jedoch im Sinne der Plattformunabhängigkeit zukünftig anzustreben. Insofern kommt hierbei den zukünftigen Aktivitäten der IETF eine maßgebliche Rolle (vgl. insofern Abschnitt 3.1.3).

Ergebnis: Insgesamt hat sich gezeigt, dass die Architektur die verfolgten Ziele erfüllt und das Einsatzspektrum von P2P-Systemen deutlich erweitert wird, da P2P-Technologien nun auch für komplexe Anwendungsszenarien nutzbar sind.

Vorteilhaft ist dabei vor allem die Dezentralisierung in Verbindung mit der Selbstorganisation, die bei klassischen Middleware-Architekturen und auch bei dienstorientierten Architekturen nicht gegeben sind. Wie die Architektur zeigt, kann P2P-Technologie somit eine gewinnbringende Ergänzung zu klassischen Architekturen für verteilte Systeme darstellen. Im Übrigen erlaubt das entwickelte Rahmenwerk auch eine kosteneffiziente Realisierung von verteilten Systemen, da durch die P2P-Technologie vorhandene brachliegende Ressourcen besser genutzt werden können.

Auch die Anforderungen des Anwendungsszenario "dezentrale elektronische Marktplattform" aus Abschnitt 4.1.1 werden erfüllt. Die Plattform kommt ohne zentrale Komponenten aus und somit ist auch kein dedizierter Betreiber notwendig. Die zur Verfügung stehenden P2P-Module ermöglichen es Dienste zu entwickeln, die skalierbar hinsichtlich Teilnehmerzahl und robust gegenüber dem Ausfall von Knoten sind. Durch den Einsatz der Web Services-Techniken ist das Rahmenwerk modular und plattformunabhängig. Insofern kann auch die Wiederverwendung von Diensten und P2P-Modulen gewährleistet werden. Die übrigen Anforderungen hinsichtlich gezielten Angriffen auf P2P-Systeme und die rechtliche Einordnung sind unabhängig von diesem Rahmenwerk und werden in den Kapiteln 5 und 6 vertieft behandelt.

Im Rahmen der prototypischen Implementierung erwies sich insbesondere die Trennung von P2P-Netzen und Diensten als sehr hilfreich, da die Dienstentwickler ihr domänenspezifisches Wissen einbringen konnten, ohne ein tiefgreifendes Verständnis von P2P-Netzen aufbringen zu müssen.

4.1.6 Resümee

Das Potential, das von P2P-Systemen für zukünftige verteilte Systeme ausgeht, wurde ausgehend von dem Anwendungsszenario "elektronischer Marktplatz" untersucht. Dabei zeigte sich, dass klassische Architekturen für verteilte Systeme Defizite hinsichtlich der Dezentralität und Selbstkonfiguration aufweisen. P2P-Systeme zeigten sich als gut vertikal integriert, d.h. für ein dediziertes Anwendungsszenarien gut geeignet. Es mangelt ihnen jedoch an einer horizontalen Integration, so dass ein Einsatz in komplexen Anwendungsszenarien schwer fällt.

Durch die Entwicklung einer *dienstorientierten P2P-Architektur* ist es gelungen, die Vorteile von dienstorientierten Architekturen mit denen von P2P-Systemen zu verknüpfen und somit die spezifischen Defizite zu kompensieren. Insgesamt konnte das Einsatzspektrum von P2P-Systemen wesentlich erweitert werden. Außerdem lässt die vorgestellte Architektur eine einfache Integration mit klassischen verteilten Systemen zu, da erprobte Web Services-Technologie zum Einsatz kommt.

4.2 Dezentrales Bootstrapping mittels kollaborativer P2P-Architektur

Die Tauglichkeit von P2P-Systemen für große bis hinzu zu sehr großen Nutzergruppen konnte sowohl wissenschaftlich als auch durch reale Systeme im Internet gezeigt werden. Fraglich bleibt jedoch, ob P2P-Systeme ihr Potential auch bei kleinen Nutzergruppen entfalten können. Diese P2P-Systeme mit wenigen Teilnehmern werden im Folgenden als *Mikro-P2P-Systeme* bezeichnet. Bei diesen steht weniger die Skalierbarkeit, denn die Robustheit gegenüber Ausfällen einzelner Knoten im Vordergrund, d.h. die Unabhängigkeit von zentraler Infrastruktur. Da ein P2P-System selbst vollständig dezentral realisiert werden kann, besteht die Herausforderung darin, einen anderen Knoten, d.h. einen Eintrittspunkt, in das P2P-System zu finden. Wie im Abschnitt 4.2.2 noch näher ausgeführt wird, werden hierzu in der Regel (zentrale) Bootstrap-Server eingesetzt deren Adresse den Knoten wohlbekannt ist.

Wenn ein solcher Server betrieben werden muss, stellt sich aus Betreibersicht somit die Frage, ob der Einsatz von P2P-Technologien überhaupt zielführend ist, da notwendige Funktion zentral meist einfacher realisiert werden können und die die erhofften Attribute wie Ausfallrobustheit nur bedingt gewährleistet sind.

Im folgenden Abschnitt wird ein Anwendungsszenario erläutert anhand dessen diese Beitrittsproblematik offensichtlich wird. Anschließend werden die Hintergründe zu Beitrittsverfahren erläutert und eine kollaborative Architektur aufgezeigt, durch welche ein vollständig dezentrales Bootstrapping möglich ist. Die Kernidee dieser kollaborativen Architektur besteht darin, dass öffentlich zugängliche P2P-Systeme mit sehr vielen Mitgliedern für die Ablage von Information genutzt werden. Durch eine umfangreiche empirische Studie in dem weit verbreiteten P2P-System BitTorrent wird gezeigt, dass sich der Ansatz in Verbindung als tragfähig erweist. Ferner wird ein wahrscheinlichkeitstheoretisches Modell aufgezeigt, mittels dessen das Beitrittsverfahren optimiert und auch die Eignung von weiteren öffentlichen P2P-Systemen beurteilt werden kann. Außerdem wird ein Verfahren für zukünftige P2P-Systeme entwickelt, welches den Beitritt wesentlich beschleunigt.

4.2.1 Anwendungsszenario: Autonomes Kommunikationssystem

Die Netzinfrastruktur des Internet wurde mit dem Fokus auf Dezentralität und somit auch Ausfallrobustheit gestaltet [Clark 1988]. Wie bereits in den vorigen Kapiteln dargelegt wurde, ist die Dezentralität bei Client/Server-Systemen auf

Anwendungsebene jedoch nicht mehr gegeben.

Ziel des Projektes *Kommunikation mittels autonomer Infrastrukturen (KAI)* [WWW Prj Kai] ist es, eine Kommunikationssystem auf Basis des Internet zu entwickeln, welches ohne zentrale Infrastrukturelemente auf Anwendungsebene auskommt. Solche zentralen Infrastrukturelemente sind klassischerweise Server, deren Adresse allen Peers bekannt ist wie zum Beispiel SMTP- oder SIP-Server. Als "zentraler Anlaufpunkt" sorgen diese für die Koordination zwischen den Knoten.

Elementare Annahme für das Kommunikationssystem ist: Teilnehmer verfügen über einen (beliebigen) Zugang zum Internet, so dass auf IP-Ebene die Möglichkeit zur Kommunikation zwischen den Teilnehmern besteht. Da es sich um beliebige Internet-Anschlüsse handeln kann, scheidet eine statische Vergabe von IP-Adressen oder Kommunikation mittels Multi- bzw. Anycast-Protokollen aus[4].

Die größte Herausforderung besteht insofern in der Lokalisierung von anderen Teilnehmern, da sich diese grundsätzlich hinter einer beliebigen IP-Adresse befinden können. Dabei ist die Anforderung zu berücksichtigen, dass sich zwei Teilnehmer, die zur selben Zeit aktiv sind, innerhalb kurzer Zeit (in weniger als 15 Minuten) finden sollen und insofern eine Durchsuchung des kompletten IP-Adressraumes ausscheidet, da der Raum potentieller IPv4-Adressen sehr groß ist (ca. 3 Milliarden allokierte IPv4-Adressen[5]). Weiterhin ist davon auszugehen, dass ein Großteil der Teilnehmer über Zugangstechniken wie DSL mit dem Internet verbunden sind, so dass die Implikationen, welche insbesondere durch NAT-Router entstehen können, Berücksichtigung finden müssen.

Die nachfolgende Kommunikation innerhalb des dedizierten KAI-Kommunikationssystems, einem Mikro-P2P-System, soll nur für authentifizierte Teilnehmer möglich sein sowie integer und vertraulich stattfinden. Für die letztgenannten Aspekte können bekannte Mechanismen eingesetzt werden, so dass diese Gesichtspunkte im Folgenden nicht weiter ausgeführt werden.

4.2.2 Hintergrund

Bootstrapping beschreibt im Wesentlichen den Prozess einen neuen Knoten in ein P2P-System zu integrieren [Karbhari et al. 2004]. Das Bootstrapping-Problem muss gelöst werden, ungeachtet dessen ob es sich um ein DHT-basiertes oder unstrukturiertes P2P-Netz handelt. Für den Beitritt zu einem P2P-System wird mindestens ein aktives Peer benötigt, d.h. ein Knoten, der gerade am P2P-System

[4]Momentan ist eine flächendeckende Verfügbarkeit von IPv6 noch nicht gegeben. Daher wurde die Studie aus Sicht von IPv4 durchgeführt. Außerdem ist zum jetzigen Zeitpunkt unklar, wie sich die Ausgestaltung, wie zum Beispiel hinsichtlich unterstützter (Multicast-)Protokolle, solcher Netze in der Praxis sein wird.

[5]Die Anzahl vergebener IP-Adressen bezieht sich auf IP-Adressbereiche, die von der IANA vergeben wurden bzw. selbst verwaltet werden (vgl. [IANA IPv4], Stand: Mai 2008).

teilnimmt. Die aktuelle Adresse (bestehend aus IP-Adresse und Port) des aktiven Peers wird im Folgenden als **Verbindungsinformation** bezeichnet. Wenn eine oder mehrere Verbindungsinformation gefunden wurden, sendet der beitretende Knoten eine entsprechende Nachricht an einen der Knoten. Die folgende Integration in das P2P-Netz erfolgt entsprechend den Mechanismen des jeweiligen P2P-Netzes. Die für das Auffinden aktiver Knoten vorgeschlagenen Mechanismen können nach [Cramer et al. 2004] in folgende Kategorien unterteilt werden:

- **Out-of-Band Mechanismen:** Als Gnutella im Jahr 2000 startete, wurden die Verbindungsinformation von aktiven Peers mittels IRC ausgetauscht [Kan 2001]. Des Weiteren wurden Websites als Out-of-Band Mechanismen genutzt [Gnutella WebCache; Karbhari et al. 2004].

- **Dedizierte Bootstrap-Server:** Viele aktuelle P2P-Systeme wie BitTorrent nutzen ein oder mehrere (zentrale) Bootstrap-Server, wobei die DNS-Namen oder IP-Adressen dieser Server allen Peers bekannt sind. Will ein Knoten dem P2P-System beitreten, kontaktiert dieser zunächst den Bootstrap-Server, welcher dann Verbindungsinformationen von gerade aktiven Peers zurückgibt.

  Selbst wenn mehrere Bootstrap-Server existieren, können diese Ziel eines Denial-of-Service-Angriffs sein und stellen somit Single-Point-of-Failures dar, da bei einem Ausfall keine Knoten dem P2P-System mehr beitreten können. Dies wurde (indirekt) offensichtlich, als die Skype Login-Knoten überlastet wurden und ein Beitritt zu Skype nicht mehr möglich war (vgl. [Arak 2007]). Zudem ist die Skalierbarkeit der Bootstrap-Server begrenzt und muss der Nutzerzahl sowie der Wechselrate der Knoten (engl. Churn-Rate) angepasst werden.

- **Lokaler Host-Cache:** Um Knoten, die bereits zuvor Teil eines P2P-Systems waren, einen schnellen Wiedereintritt zu ermöglichen, pflegen die Knoten eine Liste mit Verbindungsinformationen anderer Knoten (vgl. u.a. [Chawathe et al. 2003]). Diese Liste wird als lokaler Host-Cache bezeichnet [Baset & Schulzrinne 2006] und kann direkt aus der P2P-spezifischen Routing-Tabelle gewonnen werden. Will ein Knoten anschließend dem P2P-System wieder beitreten, versucht er einen der Knoten des Host-Cache zu kontaktieren. Dieser Ansatz bedingt jedoch, dass ein Knoten mindestens einmal mit dem P2P-System verbunden sein musste. Ferner muss auch wenigsten ein Knoten unter der gespeicherten Verbindungsinformation noch erreichbar sein. Insofern kommt der durchschnittlichen Lebenszeit von Knoten, d.h. der Zeit, in der Knoten unter der gleichen IP-Adresse und Port erreich-

bar sind, eine entscheidende Bedeutung zu, um die Leistungsfähigkeit des Host-Cache zu bewerten (vgl. auch Abschnitt 4.2.4).

– **Zufällige Adressprüfung (engl. Random Address Probing):** Ein Ansatz, ohne Unterstützung zentraler Infrastruktur oder eines lokalen Host-Cache Peers einen Beitritt in ein P2P-System zu ermöglichen, besteht darin, zufällige Verbindungsinformationen zu generieren und damit einen Beitritt durch Versenden von so genannten Probe-Nachrichten zu versuchen (engl. Probing). Insbesondere bei weit verbreiteten Systemen mit Millionen von Teilnehmern besteht die Chance innerhalb kurzer Zeit ein Peer zu finden.

  In die Verbindungsinformationen fließen die beiden Parameter IP-Adresse und Port ein. Durch geschickte Wahl der Parameter bzw. Eingrenzung der Parameterräume kann der Suchraum begrenzt werden. So existiert bei einigen P2P-Systemen bspw. ein Port, welcher standardmäßig von realisierenden P2P-Anwendungen verwendet wird. Die benötigte Zeit um ein Peer zu finden, hängt dabei von zwei Faktoren ab. Zum einen ist die Anzahl und Verteilung der Peers über den Adressraum entscheidend. In [Conrad & Hof 2007] wurde bspw. gezeigt, dass der Anteil von eMule-Peers in Zugangsnetzen (engl. Dial-Up Networks) erhöht ist. Zum Zweiten ist die benötigte Zeit auch abhängig von der Suchrate, d.h. der Anzahl (zufällig gewählter) Verbindungsinformationen, die pro Zeiteinheit überprüft werden. Die maximale Suchrate wird offensichtlich von der zur Verfügung stehenden Bandbreite begrenzt. Die Suchrate ist aber auch Beschränkungen unterworfen, die durch NAT-Router verursacht werden, wie im Anhang A gezeigt wird.

– **Protokolle und Mechanismen auf Netzwerkebene:** Neben den erläuterten Ansätzen auf Anwendungsebene, könnten auch Mechanismen auf Netzwerkebene wie zum Beispiel Multicast oder Anycast (vgl. u.a. [RFC 4291]) oder das Service Location Protocol (SLP) [Guttman 1999] für das Bootstrapping genutzt werden. Allerdings erfordern solche Protokolle eine Speicherung von Informationen in Multicast- bzw. Anycast-fähigen Routern oder zentralisierten SLP-Verzeichnissen, so dass Fragen hinsichtlich Skalierbarkeit aufgeworfen werden. Außerdem ist die Unterstützung durch die Netzinfrastruktur des Internet auf globaler Ebene nicht gegeben.

In [Castro et al. 2002b], [Jelasity et al. 2006] und [Conrad & Hof 2007] werden universelle Bootstrapping-Dienste vorgeschlagen mittels derer ein Beitritt in spezifische P2P-Systeme möglich ist, wobei die Bootstrapping-Dienste selbst wiederum als P2P-Netz organisiert sind. Für den Beitritt zum Bootstrapping-Dienst werden in [Castro et al. 2002b] und [Jelasity et al. 2006] Multicast oder wohlbe-

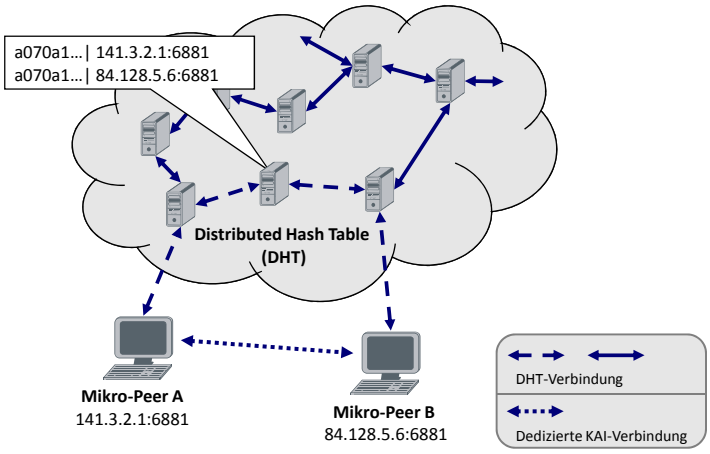


Abbildung 4.8: Skizzierung der kollaborativen P2P-Architektur

kannte Adressen vorgeschlagen, während in [Conrad & Hof 2007] Random Address Probing eingesetzt wird. Allen Vorschlägen ist gemein, dass zunächst ein neues P2P-System, der Bootstrapping-Dienst, aufgebaut werden muss.

4.2.3 Kollaborative P2P-Architektur

Zur Lösung der Beitrittsproblematik wird ein zweistufiges Verfahren genutzt, dem eine kollaborative P2P-Architektur zugrunde liegt. Die grundlegende Idee dabei ist, dass die Teilnehmer zunächst versuchen einem öffentlichen und weit verbreiteten P2P-System beizutreten, um dort *Verbindungsinformationen*, d.h. ihre aktuelle IP-Adresse nebst Port, zu speichern sowie Informationen über andere Peers zu finden. In einem zweiten Schritt erfolgt anhand dieser Verbindungsinformationen der Aufbau von dedizierten Verbindungen zwischen den Teilnehmern des Mikro-P2P-Systems, den so genannten Mikro-Peers.

Für die Ablage von Verbindungsinformationen bietet sich die Nutzung von DHTs an. So können unter *einem* Schlüssel, der allen Mikro-Peers bekannt ist, die Verbindungsinformationen der aller Peers des Mikro-P2P-Systems abgelegt werden. Hierfür kann ein beliebiger Schlüssel gewählt werden. Es müssen lediglich alle Mikro-Peers den gleichen Schlüssel nutzen. Im Vergleich zu unstrukturierten Netzen bieten DHTs den Vorteil, dass vorhandene Schlüssel/Wert-Paare garantiert gefunden werden (vgl. Abschnitt 2.4.5). Um die Existenz eines geschlossenen P2P-Systems zu verschleiern, kann der Schlüssel in regelmäßigen Abständen gewechselt werden und zudem eine nachgelagerte Authentifikation der Teilnehmer erfolgen. In Abb. 4.8 ist der Aufbau dieser kollaborativen P2P-Architektur skizziert.

Für den Beitritt zur DHT werden typischerweise Bootstrap-Server genutzt.

Dies widerspricht jedoch den Anforderungen des Anwendungsszenarios in Hinblick auf vollständige Dezentralität. Im Gegensatz zur Nutzung von Bootstrap-Servern durchsucht das in dieser Arbeit vorgeschlagene Verfahren IP-Adressräume nach aktiven Knoten der DHT mittels Random Address Probing. Wird ein Knoten gefunden, tritt das Mikro-Peer mit dessen Hilfe der DHT bei und speichert seine aktuelle Verbindungsinformationen unter dem Schlüssel, der auch allen anderen Mikro-Peers bekannt ist. Anschließend fragt das Mikro-Peer regelmäßig die ebenfalls unter diesem Schlüssel gespeicherten IP-Adressen anderer Mikro-Peers ab und kann somit zu anderen Mikro-Peers dedizierte Verbindungen aufbauen.

4.2.4 Evaluierung von weit verbreiteten P2P-Systemen

Ziel dieses Abschnitts ist es, die Tauglichkeit des dargelegten kollaborativen Verfahrens zu evaluieren. Die Eignung der entwickelten kollaborativen P2P-Architektur hängt dabei insbesondere von dem weit verbreiteten P2P-System ab, d.h. der DHT, die für die Ablage des Schlüssel genutzt wird.

Im Folgenden wird eine Bewertung des Ansatzes mittels einer umfangreichen empirischen Studie vorgenommen. Für die Untersuchung wurde die BitTorrent-DHT ausgewählt. Es handelt sich dabei um die DHT-Erweiterung von BitTorrent für den Trackerless-Modus. Wie bereits in Abschnitt 2.4.4 dargelegt, basiert die DHT-Erweiterung auf dem Protokoll Kademlia und ist vom Dateiaustausch-Protokoll unabhängig[6]. Die BitTorrent-DHT eignet sich aus zwei Gründen besonders für solch eine kollaborative Architektur: Zum einen ist das BitTorrent-System sehr verbreitet und somit eine große Anzahl aktiver Knoten vorhanden. Zum anderen ist die Spezifikation des Protokolls öffentlich bekannt und dokumentiert (vgl. [BitT BEP5 2008]). Ferner sind verschiedene zueinander kompatible Implementierungen des Protokolls vorhanden.

Für den Beitritt zur BitTorrent-DHT kommt in der Regel ein Bootstrap-Server, wie `router.bittorrent.com` oder `router.utorrent.com` zum Einsatz. Da das Mikro-P2P-System jedoch unabhängig von jeglicher zentraler Infrastruktur realisiert werden soll, sollte auch für den Beitritt in die BitTorrent-DHT auf zentrale Komponenten verzichtet werden.

Insofern wird im Folgenden untersucht, wie lange ein Probing nach einem BitTorrent-Knoten dauert. Um die Suche zu beschleunigen, ist eine Kombination mit einem (lokalen) Host-Cache sinnvoll. Insofern wird auch die "Sitzungsdauer" von BitTorrent-Knoten bestimmt. Ferner ist die Dauer abhängig von der Suchrate, d.h.

[6] Aufgrund dessen ist die Bezeichnung BitTorrent-DHT-Peer korrekt, da auch Knoten ohne diese DHT-Erweiterung existieren. In der Untersuchung werden jedoch nur Knoten mit DHT-Erweiterung betrachtet und daher die verkürzende Schreibweise BitTorrent-Peer verwendet.

der Anzahl Adressen die pro Zeiteinheit überprüft werden. Mögliche Implikationen von NAT-Routern auf die maximale Suchrate werden im Anhang A dargelegt.

Knotendichte und Port-Verteilung

Die Effektivität der zufälligen Adressprüfung bestimmt sich aus drei Faktoren:

1. *Suchrate:* Die Suchrate μ entspricht der Anzahl an Verbindungsinformationen, die pro Zeiteinheit t überprüft werden.

2. *Knotendichte:* Der Erfolg der zufälligen Adressprüfung ist maßgeblich bestimmt durch die Anzahl n der Knoten des weit verbreiteten P2P-Systems im Verhältnis zur der Anzahl möglicher IP-Adressen.

3. *Port-Verteilung:* Zur Adressierung von Knoten muss auch ein UDP-Port spezifiziert werden. Insofern erweitert sich der Suchraum um die möglichen Ports.

Soweit nicht anders kenntlich gemacht, bezieht sich der Ausdruck Knoten im weiteren Verlauf dieses Kapitels auf einen Knoten des weit verbreiteten P2P-Systems.

Messaufbau: Für empirische Messungen wurde der Ping-Mechanismus des Kademlia-Protokolls genutzt. Hierzu wurde jeweils ein Kademlia-Ping-Paket an die potentielle IP-Adressen an den "Standard-UDP-Port" 6881 gesendet. Für die BitTorrent-DHT gibt es keinen wohlbekannten Port gemäß [IANA Ports]. Da jedoch der so genannte Mainline Client [WWW BitTorrent] lange standardmäßig den UDP-Port 6881 für die DHT nutzte, kann dieser als Standard-Port angenommen werden. Eine detaillierte Analyse der aktuell verwendeten Ports folgt im weiteren Verlauf dieses Abschnitts.

Wenn ein BitTorrent-Knoten solch ein Ping-Paket empfängt, sendet er eine entsprechende Antwort zurück. Aufgrund des UDP-Protokolls fand das Senden und Empfangen asynchron statt, d.h. nach dem Senden eines Ping-Pakets an eine IP-Adresse wurde nicht auf eine Antwort gewartet, sondern unmittelbar mit der nächsten IP-Adresse fortgefahren. Eingehende Antworten wurden parallel dazu verarbeitet.

Mathematische Modellierung: Zur Formalisierung wird an dieser Stelle ein mathematisches Modell eingeführt, dass sowohl zur Bewertung der Messergebnisse als auch der Optimierung der Suche dient. Es werden hierzu zunächst folgende Bezeichnungen und Symbole definiert[7]:

[7] Eine Übersicht der in dieser Arbeit verwendeten mathematischen Symbole findet sich im Anhang C.

- a entspricht der Anzahl an IP-Adressen, die potentiell für den Betrieb von Knoten in Betracht kommen.
- Durch b wird die Anzahl möglicher Ports, unter welchen ein Knoten betrieben werden kann, ausgedrückt.
- Der Suchraum Ω ergibt sich aus den potentiellen IP-Adressen und den möglichen Ports. Wenn die möglichen Ports unabhängig von den IP-Adressen sind, gilt $|\Omega| = a \cdot b$.
- k entspricht der Versuchsanzahl bei der zufälligen Adressprüfung.
- l entspricht der Anzahl der zu überprüfenden Ports je IP-Adresse.

Bei der Anzahl der Versuche k ist zu beachten, dass es unerheblich ist, ob eine andere IP-Adresse oder unter der gleichen IP-Adresse ein anderer Port überprüft wird. In jedem Fall muss ein Datenpaket versandt werden, so dass sich k um eins erhöht. Ferner gilt $l \leqslant b$, da nicht mehr Ports pro IP-Adresse überprüft werden können als vorhanden sind.

Weiterhin sollen die folgenden Wahrscheinlichkeiten definiert werden:

- $P(A)$ entspricht der Wahrscheinlichkeit, dass unter einer zufällig gewählten IP-Adresse ein Knoten betrieben wird. Für die Wahrscheinlichkeit gilt dabei: $P(A) = \frac{n}{a}$.
- $P(B_i)$ entspricht der Wahrscheinlichkeit, dass ein Knoten den Port i nutzt.
- $P(C_i)$ sei die Wahrscheinlichkeit, dass mit einer Verbindungsinformation, d.h. der Kombination aus einer IP-Adresse und einem Port i, ein Knoten gefunden wird.

  Die beiden Wahrscheinlichkeiten $P(A)$ und $P(B)$ werden als unabhängig voneinander angenommen. Daher gilt $P(C_i) = P(A) \cdot P(B_i)$.

Für die weitere Betrachtung und die Bewertung der Messung wird zunächst der Fall betrachtet, dass nur ein Port je IP-Adresse untersucht wird, d.h. $l = 1$. Die folgende Betrachtung kann daher auf Basis von $P(C_i)$ stattfinden. Die Anpassung der Suchstrategie für den Fall mehrerer Ports pro IP-Adresse wird in Abschnitt 4.2.5 und 4.2.6 diskutiert.

Wenn nur *ein* Port pro IP-Adresse überprüft wird, kann aus Sicht der Wahrscheinlichkeitstheorie die zufällige Adressprüfung als Bernoulli-Experiment modelliert werden, bei welchem ein Treffer einem gefunden Knoten entspricht. Dabei wird die Annahme zugrunde gelegt, dass die Gesamtanzahl der Knoten n konstant bleibt und der Suchraum im Verhältnis zur Suchrate sehr groß ist, so dass die Zufallsexperimente als unabhängig betrachtet werden können. Im Sinne des Urnenmodells handelt es sich bei der zufälligen Adressprüfung mit einem Port daher um ein Ziehen mit Zurücklegen.

Den Annahmen liegt dabei zugrunde, dass die Anzahl der potentiellen IP-Adressen sehr groß und die Suchrate im Verhältnis dazu relativ gering ist. Insbesondere kann es dazu kommen, dass während der zufälligen Adressprüfung ein neuer Knoten unter einer bereits überprüften IP-Adresse betrieben wird. Diese Annahme wird auch durch die folgenden Messergebnisse hinsichtlich möglicher Suchrate und Länge der Sitzungsdauer gestützt (Die Messergebnisse werden dabei nicht durch die Annahmen beeinflusst.).

Im Fall der zufälligen Adressprüfung ist vor allem die Anzahl der Versuche k von Interesse, die erforderlich ist, um einen Knoten zu finden. Die zugehörige Verteilung wird als negative Binomialverteilung $Nb(w, p)$ bezeichnet [Henze & Kadelka 2000, S. 76], wobei w der Trefferanzahl entspricht. Daher ergibt sich die Wahrscheinlichkeit nach k Versuchen genau einen Treffer zu haben zu:

$$f(k) := P(C_i) \cdot (1 - P(C_i))^k \tag{4.1}$$

Bei der zufälligen Adressprüfung ist jedoch weniger die Wahrscheinlichkeit von Belang nach k-Versuchen genau einen Treffer zu haben. Vielmehr ist die Wahrscheinlichkeit nach k-Versuchen mindestens einen Treffer zu haben für die Beurteilung des Verfahrens relevant. Diese ergibt sich aus der Verteilungsfunktion:

$$F(k) := 1 - (1 - P(C_i))^k \tag{4.2}$$

Wenn es sich um ein seltenes Ereignis handelt, kann die Häufigkeit auch durch die Exponentialverteilung näherungsweise bestimmt werden und es ergibt sich $F(k) = 1 - e^{-\lambda \cdot k}, k \geqslant 0 \text{ und } \lambda = P(C_i)$ (vgl. u.a. [Henze & Kadelka 2000, S. 88]).

Suchrate: Die Dauer der Suche ist neben der Wahrscheinlichkeit, einen Knoten zu finden, durch die Suchrate bestimmt. Die Suchrate wird dabei in pkt/s angegeben, d.h. die Anzahl unterschiedlicher Verbindungsinformationen, die pro Sekunde geprüft werden. Somit ergibt sich die Wahrscheinlichkeit innerhalb einer festgelegten Zeit t einen BitTorrent-Knoten zu finden: $F(t) = 1 - (1 - P(C_i))^{\mu \cdot t}$

Die maximal mögliche Suchrate μ ist offensichtlich, durch die zur Verfügung stehende Upstream-Bandbreite, begrenzt. Das verwendete Kademlia-Ping-Paket hat eine Größe von 65 Byte, was bei Ethernet einschließlich aller Header zu einer Größe von 107 Byte führt. Für eine Suchrate von 100 pkt/s ergibt sich somit eine notwendige Bandbreite von ca. 81 kbit/s.

Bei den Messungen hat sich allerdings gezeigt, dass die Suchrate auch durch Zwischensysteme wie NAT-Router oder Firewalls begrenzt sein kann, so dass die Suchrate teilweise deutlich, auf bis zu 35 pkt/s, reduziert wird. Eine detaillierte Darlegung dieser Problematik erfolgt im Anhang A.

Knotendichte im Internet: Für das entwickelte Verfahren ist es entscheidend wann der erste Knoten gefunden wird, da bereits ein Knoten ausreicht, um dem System beizutreten. Um die Dauer des Beitritts abschätzen zu können, ist daher die Wahrscheinlichkeit $P(C_i)$ fraglich.

Der Suchraum Ω wurde begrenzt auf den Port 6881 ($b = 1$) und die Menge der IP-Adressen, die potentiell allokiert werden können, d.h. die Menge aller IPv4-Adressen 2^{32} abzüglich der IP-Adressen, die gemäß [RFC 3330] für spezielle Zwecke vorgesehen sind. Daraus ergibt sich eine Reduktion um ca. 15 % auf $a = 3,656 \cdot 10^9$ IP-Adressen. Eine Abschätzung der Wahrscheinlichkeit $P(C_{6881})$ wurde durch Messungen ermittelt, wobei die Anzahl Treffer w nach k-Versuchen bestimmt wurde, da unter den oben genannten Annahmen $P(C_{6881}) = \lim_{k\to\infty} \frac{w}{k}$ gilt.

Die Intervallgrenzen für ein 95%-Konfidenzintervall einer Binomialverteilung können nach [Henze & Kadelka 2000, S. 180] in einer vereinfachten Form wie folgt berechnet werden:

$$l_k(X_1,\ldots,X_k) := \overline{X}_k - \frac{1,96}{\sqrt{k}} \cdot \sqrt{\overline{X}_k(1-\overline{X}_k)}$$
$$L_k(X_1,\ldots,X_k) := \overline{X}_k + \frac{1,96}{\sqrt{k}} \cdot \sqrt{\overline{X}_k(1-\overline{X}_k)}$$

Um die Knotendichte zu ermitteln wurde eine Suche nach BitTorrent-DHT-Knoten im Internet durchgeführt. Die Messungen wurden mittels eines eigens entwickelten Testprogramms im Juni 2008 aus dem Netz der Universität Karlsruhe (TH) durchgeführt, wobei der Messaufbau dem eingangs beschriebenen entsprach.

Für die Messungen wurden die Suchraten $\mu = 50\text{pkt/s}$ und $\mu = 100\text{pkt/s}$ verwendet. Tabelle 4.3 zeigt die ermittelten Ergebnisse der Messung. Aus den Messungen ergibt sich insbesondere, dass die Wahrscheinlichkeit unter einer zufällig gewählten IP-Adresse und dem Port 6881 einen BitTorrent-Knoten im Internet zu finden in etwa $P(C_i) = 3,7 \cdot 10^{-6}$ beträgt. Die Untersuchung der Port-Verteilung, die im Folgenden noch näher ausgeführt wird, ergibt, dass ca. 1,3 %

	$\mu = 50\text{pkt/s}$	$\mu = 100\text{pkt/s}$
k	27.820.393	124.845.396
$P(C_{6881})$	$3,3788 \cdot 10^{-6}$	$3,9409 \cdot 10^{-6}$
$l_k(X_1,\ldots,X_k)$	$2,6175 \cdot 10^{-6}$	$3,5926 \cdot 10^{-6}$
$L_k(X_1,\ldots,X_k)$	$4,1401 \cdot 10^{-6}$	$4,2891 \cdot 10^{-6}$

Tabelle 4.3: Knotendichte an BitTorrent-DHT-Knoten, die den Port 6881 verwenden, im Internet

der Knoten den Port 6881 nutzen, d.h. $P(B_{6881}) = 0,013$. In Verbindung mit abgeschätzten $P(C_i)$ folgt somit, dass mehr als eine Million BitTorrent-DHT-Knoten aktiv waren. Die empirischen Werte zeigen jedoch auch, dass das Ereignis, einen BitTorrent-Knoten (auf diese Weise) zu finden, äußerst selten ist. Bei einer Suchrate von 100 pkt/s finden sich durchschnittlich ca. 1,41 BitTorrent-Knoten pro Stunde.

Knotendichte in Zugangsnetzen: Da vor allem im Bereich von Zugangsnetzen eine erhöhte Zahl von Peers und somit auch BitTorrent-Knoten zu erwarten ist [Conrad & Hof 2007], wurden in einer zweiten Messreihe solche Netze durchsucht. Hierzu wurde eine Liste mit 29.014 Class-C-Netzen[8] genutzt, bei denen es sich (mit großer Wahrscheinlichkeit[9]) um Zugangsnetze handelt.

Bei den Messungen wurden jeweils alle 29.014 Class-C-Netze durchsucht, was mehr als 7 Millionen IP-Adressen entspricht. Die IP-Adressbereiche wurden dabei sequentiell durchsucht und als Port 6881 gewählt. Es wurde jeweils protokolliert, wie viel Zeit verstrichen ist bzw. Versuche nötig waren, bis der nächste Knoten gefunden wurde. Den Suchläufen lag jeweils eine Suchrate von $\mu = 100\mathrm{pkt/s}$ zugrunde.

Abb. 4.9 zeigt die experimentell ermittelten Messreihen als kumulative Verteilungsfunktion (engl. Cumulative Distribution Function, CDF), wobei auf der x-Achse die Zeit in Minuten aufgetragen ist und auf der y-Achse die Wahrscheinlichkeit, dass ein Peer innerhalb dieser Zeit gefunden wird. In Abb. 4.9 ist der Durchschnitt von 12 unterschiedlichen Suchläufen einschließlich 95%-Konfidenzintervall dargestellt. Dabei zeigt sich, dass in allen Suchläufen bei einer Suchrate von 100 pkt/s nach 12 Minuten mit einer Wahrscheinlichkeit von 95 % ein BitTorrent-Knoten gefunden wurde.

Die Abbildung zeigt auch die Verteilungsfunktion $F(k)$ gemäß des Terms (4.2) mit einer Wahrscheinlichkeit $P(C_{6881}) = 0,173$, die sich als Mittelwert aus den Messungen ergeben hat. Dabei wird deutlich, dass die gemessene Verteilung vor allem zu Beginn deutlich besser ist als die zu erwartende Verteilung. Dies ist bedingt durch die sequentielle Suche in den Zugangsnetzen in Verbindung mit einer ungleichen Verteilung der BitTorrent-DHT-Knoten über die durchsuchten IP-Adressbereiche. Abb. 4.10 zeigt hierzu die Anzahl der gefunden BitTorrent-DHT-Knoten im Vergleich zur Suchdauer. Bedingt durch die sequentielle Suche ergibt sich somit die Verteilung der BitTorrent-DHT-Knoten über die durchsuchten IP-Adressbereiche. Der steile Anstieg der Kurve gegen Ende des betrachteten Intervalls zeigt, dass in diesem Bereich eine höhere Knotendichte gegeben ist.

[8] Die Liste entspricht der in [Conrad & Hof 2007].

[9] Eine explizite Kategorisierung von Zugangsnetzen ist nicht möglich. Die genannte Liste wurde empirisch ermittelt.

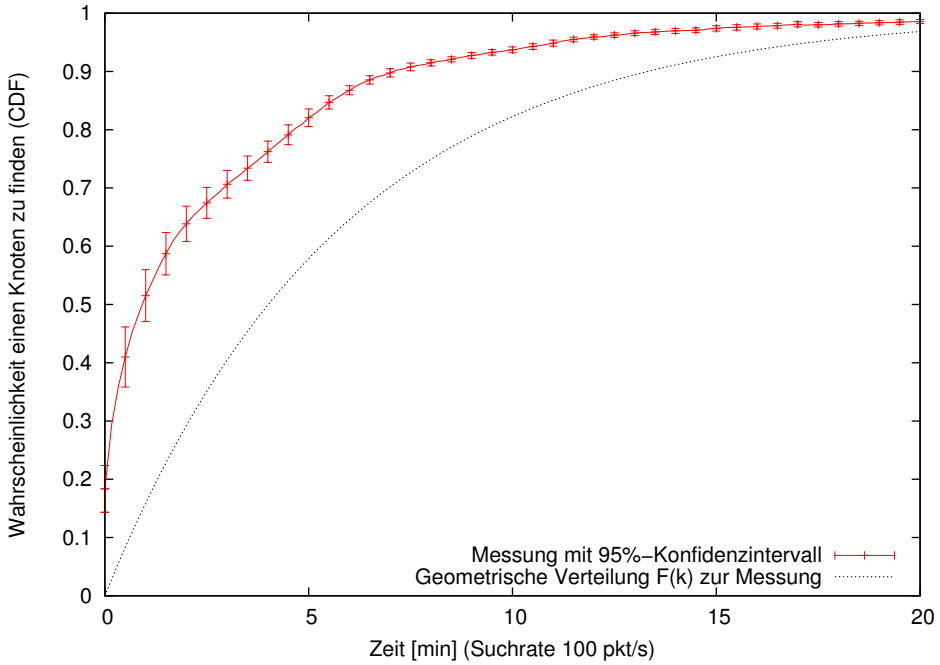


Abbildung 4.9: Suchdauer nach einem BitTorrent-DHT-Knoten in Zugangsnetzen bei einer Suchrate von 100 pkt/s dargestellt als CDF

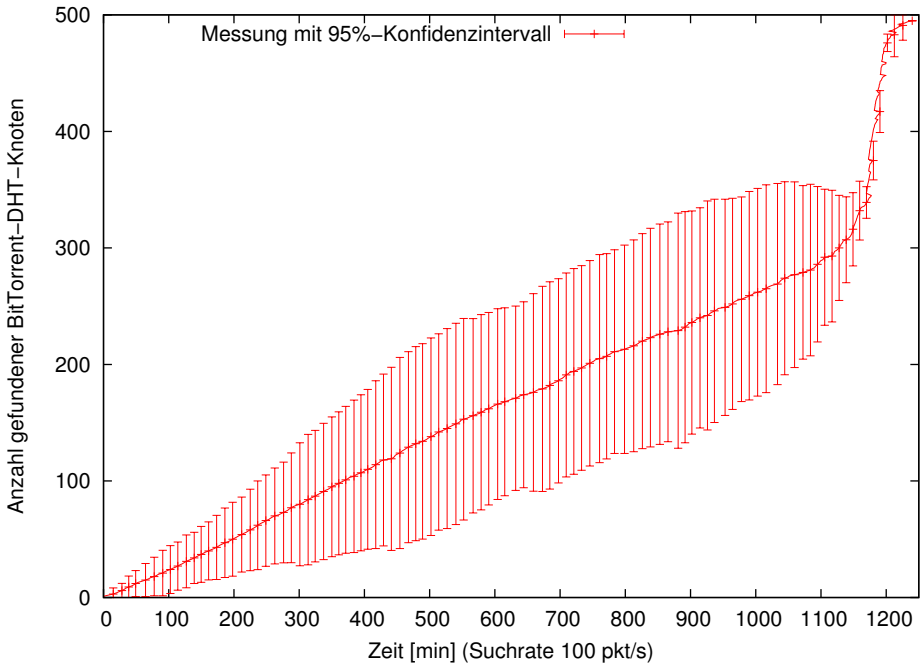


Abbildung 4.10: Anzahl der gefunden BitTorrent-DHT-Knoten in Zugangsnetzen im Vergleich zur Suchdauer bei einer Suchrate von 100 pkt/s

Port-Verteilung: Der so genannte Mainline Client von BitTorrent nutzte bis zur Version 5.2.0 standardmäßig den UDP-Port 6881 für die BitTorrent-DHT. Mit der Umstellung auf Version 6.0 wurde µTorrent als Basis des neuen Mainline Clients gewählt und der Port wird seither zufällig bei der Installation gewählt. Insofern ist zu erwarten, dass sich die Suchdauer zukünftig verlängern wird.

Zur Ermittlung der Port-Verteilung wurde eine Messung innerhalb der BitTorrent-DHT durchgeführt. Zunächst erfolgte ein Beitritt in die DHT und im zweiten Schritt wurde nach zufälligen Schlüsseln mit einer Rate von einem Schlüssel pro Sekunde gesucht.

Durch die Messung wurden über einen Zeitraum von 8 Tagen im April 2008 ca. 5,2 Millionen Verbindungsinformationen (IP-Adresse und UDP-Port) ermittelt, die als Antwort auf die Anfragen von anderen Knoten zurück gesendet wurden. Abb. 4.11 zeigt die resultierende Verteilung als Histogramm. Dabei treten zwei Spitzen hervor, wobei die erste dem Port 6881 und die zweite dem Port 16.001 entspricht. Die erste Spitze resultiert von dem "ehemaligen Standard-Port". Dieser wird durchschnittlich noch von ca. 1,3 % der Knoten genutzt. Bei näherer Analyse der zweiten Spitze hat sich ergeben, dass diese überwiegend durch einen Client aus dem chinesischen Raum bestimmt wird[10]. Hierzu wurde mittels der MaxMind GeoIP Datenbank [WWW MaxMind] eine Zuordnung von IP-Adressen zu Ländern vorgenommen. Abb. 4.12 zeigt diese Zuordnung, wobei nur die Top 15 berücksichtigt wurden. Dabei zeigt sich, dass der fragliche Port 16.001 hauptsächlich von Clients in China (ca. 90 %), Taiwan (ca. 4 %) und Hong Kong (ca. 1 %) genutzt wird. Die Abb. 4.12 zeigt darüber hinaus, dass bei dieser Messung über alle Ports gesehen 23 % aller Peers in China 10 % in den USA und 2,2 % in Deutschland beheimatet sind.

Um die Auswirkung der Port-Verteilung für die zufällige Adressprüfung bewerten zu können, bietet sich die Bestimmung der Entropie an. Bei einer niedrigen Entropie ist die Port-Verteilung dabei gering, so dass eine zielgerichtete Suche leichter fällt. Fasst man die Ports als Alphabet $\{x_0, \ldots, x_{65.535}\}$ auf und $p(x_i) = P(B_i)$ als die Wahrscheinlichkeit, dass ein Client den Port i nutzt, ergibt sich die Entropie durch (4.3). Bei einer Gleichverteilung folgt somit die maximale Entropie durch (4.4):

$$H_Q = -\sum_{i=0}^{65.535} p(x_i) \cdot \log_2 p(x_i) \tag{4.3}$$

$$H_{QMax} = -\sum_{i=0}^{65.535} \frac{1}{65.535} \cdot \log_2 \frac{1}{65.535} = 16 \tag{4.4}$$

[10] Eine genauere Identifizierung des Clients ist nicht möglich, da dieser keine Kennung in den Datenpaketen hinterlegt (vgl. hierzu [WWW libTorrent a]).

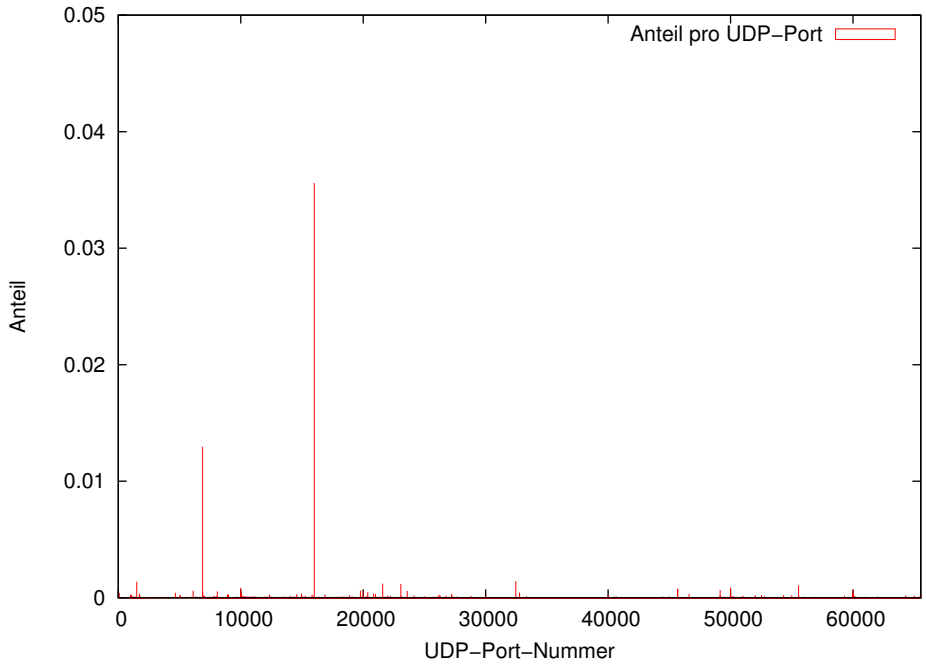


Abbildung 4.11: Port-Verteilung: Anteil der BitTorrent-DHT-Knoten pro UDP-Port, der sich aus 5,2 Millionen Datensätzen ergibt

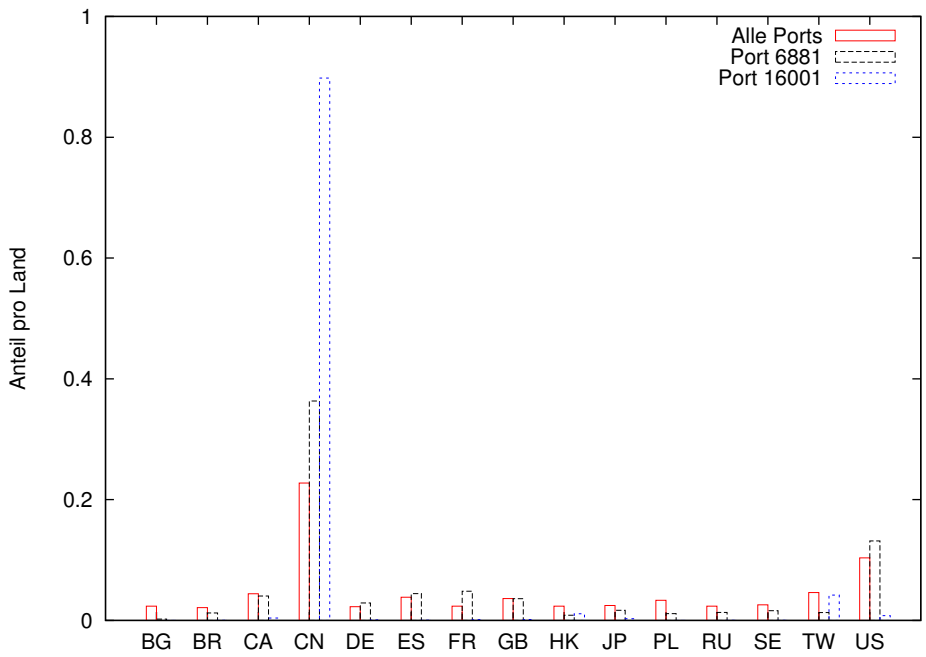


Abbildung 4.12: Zuordnung von BitTorrent-DHT-Knoten zu Ländern

Für die gemessene Verteilung ergibt sich die Entropie zu ca. $H_Q = 15,17$, welche der maximalen Entropie sehr nahe kommt. Dies verdeutlicht, dass der Einfluss der beiden Spitzen relativ gering und im Wesentlichen eine Gleichverteilung gegeben ist (vgl. auch Abschnitt 4.2.6).

Sitzungsdauer von BitTorrent-DHT-Knoten

Die Suche nach BitTorrent-Knoten wird zum einen durch NAT-Router stark eingeschränkt (vgl. Anhang A). Wie im vorigen Abschnitt erläutert, wird die Suche aber auch durch die Tatsache erschwert, dass aktuelle Implementierung keinen "Standard-Port" mehr nutzen und die Entropie der Port-Verteilung sehr hoch ist. Diese Gesichtspunkte führen dazu, dass die Suche nach einem BitTorrent-Knoten wesentlich verlangsamt wird.

Daher kann das vorgeschlagene Verfahren insoweit angepasst werden, dass jeder Teilnehmer des Mikro-P2P-Systems regelmäßig der BitTorrent-DHT beitritt und eine Liste mit Verbindungsinformationen speichert, d.h. einen lokalen Host Cache aufbaut. Diese Liste kann bei einem späteren Wiedereintritt genutzt werden, so dass kein Probing erfolgen muss, sondern gezielt mögliche BitTorrent-Knoten kontaktiert werden können.

Für die Effektivität des Bootstrapping mittels eines solchen Host Cache ist es entscheidend, wie lange die Knoten unter der bekannten Verbindungsinformation (IP-Adresse und UDP-Port) erreichbar sind. Diese Zeit wird im Folgenden als *Sitzungsdauer* eines Knotens bezeichnet. Im Gegensatz zu anderen Arbeiten wie [Steiner et al. 2007], welche die Sitzungsdauer eines Knotens anhand der DHT-spezifischen Kennung ermitteln, ist für dieses Verfahren lediglich die Zeit relevant, die ein Knoten über die gleiche Adresse erreichbar ist.

Die Sitzungsdauer der Knoten wurde ermittelt, indem der exemplarisch gewählte IP-Adressbereich 84.128.x.x - 84.144.x.x (ein Zugangsnetz der Deutschen Telekom AG) ständig nach BitTorrent-DHT-Knoten durchsucht wurde. Bekannten Knoten wurde alle 3 Minuten ein weiteres Kademlia-Ping-Paket zugeschickt. Wenn ein Knoten auf fünf aufeinander folgende Kademlia-Pings nicht antwortete, d.h. nach 15 Minuten, wurde er für inaktiv erklärt. Die Schranke von 15 Minuten wurde entsprechend der BitTorrent-DHT-Spezifikation [BitT BEP5 2008] gewählt.

Bei der ermittelten Sitzungsdauer handelt es sich um eine untere Schranke, im Folgenden als *minimale Sitzungsdauer* bezeichnet, da die Knoten in der Regel mit BitTorrent verbunden sind, bevor sie zum ersten Mal durch die Suche entdeckt werden.

Abb. 4.13 zeigt die Verteilung der minimalen Sitzungsdauer als so genannte Complementary Cumulative Distribution Function (CCDF), d.h. auf der x-

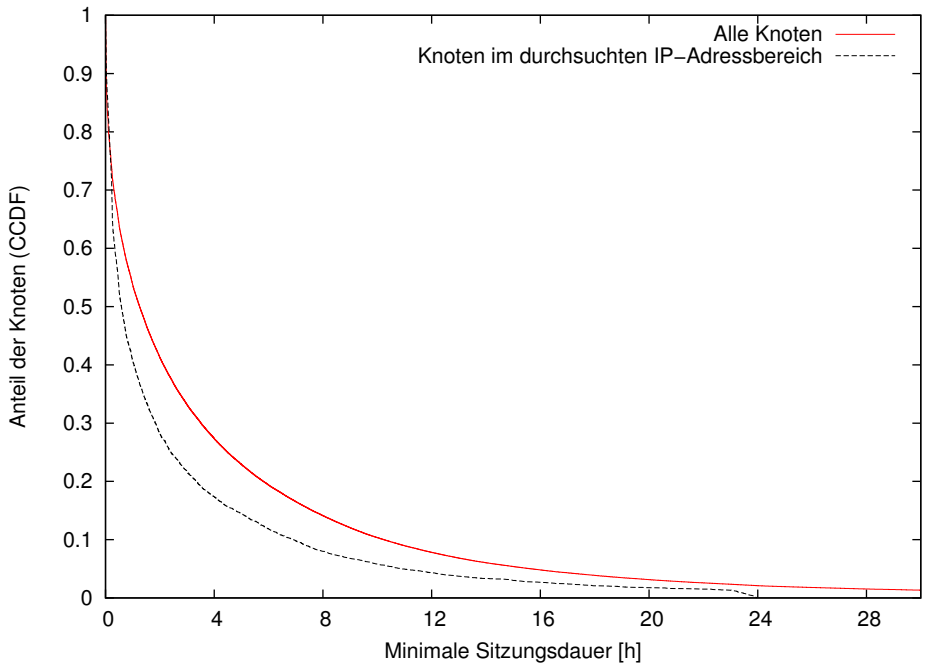


Abbildung 4.13: Verteilung der minimalen Sitzungsdauer von BitTorrent-DHT-Knoten als komplementäre CDF (CCDF)

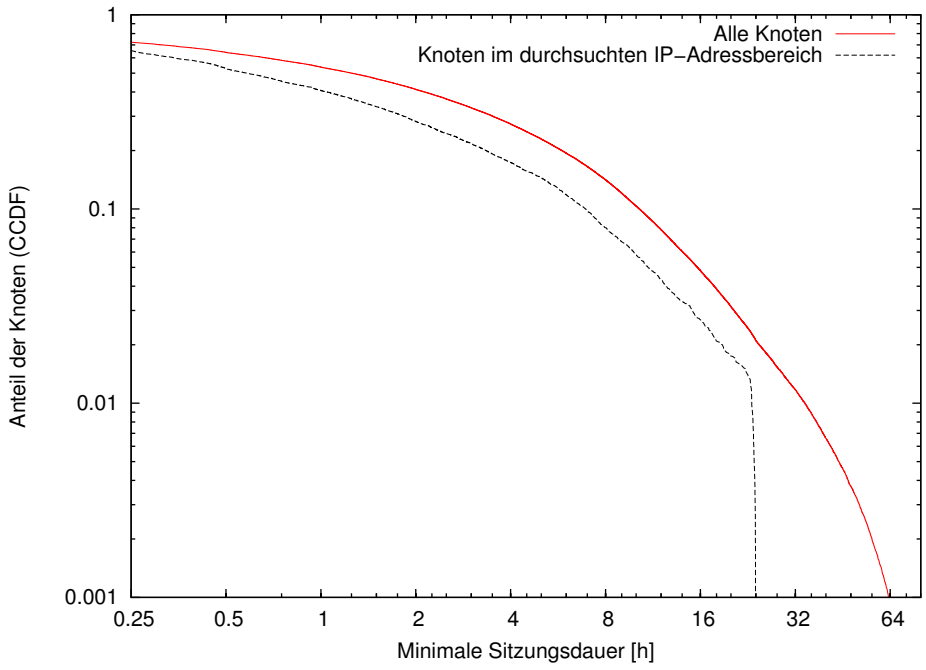


Abbildung 4.14: Verteilung der minimalen Sitzungsdauer von BitTorrent-DHT-Knoten als komplementäre CDF (CCDF) in logarithmischer Darstellung

Achse ist die minimale Sitzungsdauer in Stunden aufgetragen und auf der y-Achse die Wahrscheinlichkeit, dass ein Knoten noch unter der bekannten Adresse erreichbar ist. Die Kurve "Knoten im durchsuchten IP-Adressbereich" wurde im IP-Bereich 84.128.x.x - 84.144.x.x ermittelt, wobei der Bereich ständig mit einer Suchrate von 300 pkt/s über 25 Tage hinweg im März 2008 durchsucht wurde. Die komplette Durchsuchung des IP-Bereichs dauerte ca. 58 Minuten. Insofern ist die Sitzungsdauer eines Knotens maximal 58 Minuten länger, als die gemessene Zeit. Außerdem werden Knoten, die weniger als 58 Minuten online sind, unter Umständen nicht erfasst. Die Verteilung von "Knoten im durchsuchten IP-Adressbereich" zeigt, dass ca. 8 % der erfassten Knoten mehr als 8 h online sind. Weiterhin ist erkennbar, dass es sich um ein Zugangsnetz handelt, in welchem nach 24 h eine Zwangstrennung erfolgt. Dieser Effekt ist in Abb. 4.14 durch die logarithmische Darstellung noch deutlicher zu erkennen.

Die zweite Kurve "Alle Knoten" beinhaltet zusätzlich BitTorrent-Knoten aus anderen IP-Bereichen, die sich nicht im durchsuchten IP-Bereich befanden, sondern Kontakt zum Messknoten aufnahmen, weil Knoten aus dem durchsuchten IP-Bereich die Adresse des Messknotens weitergaben. Über die gesamte Zeit wurden 6.449 Verbindungsinformationen von Knoten in dem durchsuchten IP-Bereich und insgesamt 238.628 Verbindungsinformationen registriert, d.h. die Anzahl der Knoten, die den Messknoten von sich aus kontaktierten, ist wesentlich größer als die Anzahl aktiv gesuchter Knoten. Dabei ist zu berücksichtigen, dass bei den zusätzlichen Knoten der Erkennungsfehler größer als 58 Minuten sein kann. Dennoch ist die Sitzungsdauer, über alle Knoten hinweg gesehen, größer als im durchsuchten IP-Bereich. Bei den zusätzlichen Knoten ist auch erkennbar, dass mehr als 2% von diesen länger als 24 h unter der gleichen Adresse erreichbar sind. In den Messdaten fanden sich einige Knoten, die über 7 Tage unter der gleichen Adresse erreichbar waren. Dabei wurden nur Knoten berücksichtigt, die mindestens eine Sekunde aktiv waren. Hierdurch wurden Knoten ausgefiltert, von welchen ein Paket empfangen wurde, die selbst jedoch nicht auf Pings antworten (z.B. aufgrund von Firewalls).

Zusammenfassend lässt sich sagen, dass nach ca. 23 h noch ca. 1,3 % der Knoten im durchsuchten IP-Adressbereich erreichbar waren. Über alle Knoten hinweg waren ca. 0,1 % der Knoten mindestens 64 h unter der gleichen Adresse erreichbar. Ist ein Mikro-Peer in der BitTorrent-DHT aktiv, kann er sich sehr einfach eine Liste mit mehreren hundert oder tausend Knoten zusammenstellen. Nutzt der Mikro-Peer nach einigen Stunden oder Tagen diese Liste zum Wiedereintritt, kann mit hoher Wahrscheinlichkeit davon ausgegangen werden, dass noch mindestens ein Knoten unter der gleichen Adresse erreichbar ist. So ergibt sich bei einer Wahrscheinlichkeit p_{life} für eine ausreichend lange Sitzungsdauer

und eine Listenlänge x die Erfolgswahrscheinlichkeit aus: $1 - (1 - p_{life})^x$.

Entsprechend der empirisch ermittelten Wahrscheinlichkeit $p_{life} = 0,001$ (vgl. Abb. 4.14) für eine Sitzungsdauer von mehr als 64 Stunden und eine Liste mit 1.000 Einträgen ergibt sich eine Erfolgswahrscheinlichkeit von 63 %. Für 10.000 Einträge beträgt die Wahrscheinlichkeit, dass ein Knoten des Host Cache noch erreichbar ist sogar 99,996 %. Da selbst bei einer niedrigen Suchrate von 30 pkt/s 10.000 IP-Adressen in weniger als 6 Minuten durchsucht werden können, ist somit auch nach 64 Stunden ein Beitritt in die BitTorrent-DHT im Durchschnitt wesentlich schneller als durch Probing möglich.

Vergleich mit verwandten Arbeiten

Im Rahmen von [Stutzbach & Rejaie 2006a] und [Steiner et al. 2007] wurde das KAD-Netz, welches auch auf dem DHT-Protokoll Kademlia basiert, untersucht. Dabei wurden mehrere Millionen gleichzeitig aktiver Knoten festgestellt [Steiner et al. 2007]. Der Fokus der Arbeiten lag jedoch nicht auf der Beitrittsproblematik, weshalb insbesondere die Sitzungsdauer nicht in Bezug auf IP-Adressen ermittelt wurde. Vielmehr wurde die Sitzungsdauer anhand der DHT-spezifischen Kennungen bestimmt, d.h. die IP-Adresse konnte sich während einer Sitzung ändern. In [Stutzbach & Rejaie 2006b] wurde die Sitzungsdauer von Knoten für die P2P-Netze Gnutella, KAD und BitTorrent (im Tracker-Modus) bestimmt. Trotz der verschiedenen Messmethodik zeigen sich bei logarithmischer Darstellung große Übereinstimmungen mit den im vorigen Abschnitt beschriebenen Messungen.

Eine alternative DHT für BitTorrent wird durch den verbreiteten BitTorrent-Client Azureus aufgebaut. In [Falkner et al. 2007] wurde der Aufbau dieser DHT untersucht, wobei die Messungen hinsichtlich der Sitzungsdauer nur rudimentär durchgeführt wurden. Die Autoren argumentieren, dass sie bei der Mehrheit der Knoten eine Sitzungsdauer von mehreren Stunden vermuten, dies jedoch nicht detailliert untersucht haben.

In [Qiao & Bustamante 2006] wurde eine Messung der Sitzungsdauer von Peers in Overnet auf Basis von IP-Adresse und Port vorgenommen, wobei es sich bei Overnet auch um eine Kademlia-basierte DHT handelt. Die ermittelten Werte sind dabei ähnlich zu den hier ermittelten Werten der Sitzungsdauer über alle Peers. In Overnet hatten bspw. 50 % der Knoten eine Sitzungsdauer von weniger als 4.300 Sekunden und in der obigen Messung 4.500 Sekunden sowie 2,7 % der Knoten waren länger als ein Tag aktiv und in der BitTorrent-DHT ca. 2,1 % der Knoten.

Allen genannten Arbeiten ist gemein, dass die Messungen aus dem jeweiligen P2P-Netz heraus stattfanden und somit keine Aussagen darüber getroffen werden können, wie schnell sich Peers durch Probing finden lassen, da insbesondere die

Port-Verteilung nicht berücksichtigt wurde. Ferner wird die Sitzungsdauer meist auf Basis der DHT-spezifischen Kennung bestimmt, so dass auch diese Werte in dieser Arbeit nur bedingt Verwendung finden können.

4.2.5 Optimierung der zufälligen Adressprüfung

Bislang wurde angenommen, dass jeweils nur ein Port bei der zufälligen Adressprüfung berücksichtigt wird. Gegebenenfalls kann die Adressprüfung jedoch optimiert werden, indem bei der Suche mehrere Ports berücksichtigt werden. In diesem Abschnitt wird hierzu ein Optimierungsproblem formuliert anhand dessen die optimal zu überprüfende Port-Anzahl bestimmt werden kann, wenn die Port-Verteilung bekannt ist. Die Bestimmung der Port-Verteilung kann mittels einer Messung stattfinden, wie sie im vorigen Abschnitt beschrieben wurde.

Die Wahrscheinlichkeit, dass die Suche nach k Versuchen erfolgreich ist, wenn immer der gleiche Port i untersucht wird, ergibt sich aus der entsprechenden Formel (4.2) durch $F(k) := 1 - (1 - P(C_i))^k$. Insofern stellt sich die Frage, ob sich bei einer bekannten, als stabil angenommen Port-Verteilung eine höhere Wahrscheinlichkeit ergeben kann, wenn mehrere Ports einer IP-Adresse untersucht werden.

Bei der Adressprüfung mit unterschiedlichen IP-Adressen wurde angenommen, dass die Versuche unabhängig voneinander sind, da die Anzahl potentieller IP-Adressen (bei IPv4 im Internet ca. $a = 3,7 \cdot 10^9$) im Vergleich zur Suchrate sehr groß ist (vgl. mathematische Modellierung in Abschnitt 4.2.4).

Im Unterschied dazu kann angenommen werden, dass die Versuche bei der Überprüfung von unterschiedlichen Ports der gleichen IP-Adresse abhängig sind, d.h. im Sinne des Urnenmodells ein Ziehen ohne Zurücklegen vorliegt. Dies ist dadurch bedingt, dass das Verhältnis zwischen den möglichen Ports (bei UDP $b = 65.536$) und der Suchrate wesentlich geringer ist und somit die Knoten während der Überprüfung der Ports angenommen werden kann, dass keine Knoten dem P2P-System bei- oder austreten. Daher gilt:

$$\sum_{i=1}^{b} P(B_i) = 1$$

Offensichtlich ist die Prüfung bei wahrscheinlicheren Ports zielführender, daher wird o.B.d.A. eine Sortierung der Port-Verteilung wie folgt angenommen: $P(B_i) \geqslant P(B_j)$ für $1 \leqslant i < j \leqslant b$. Die Wahrscheinlichkeit nach k Versuchen bei l überprüften Ports ergibt sich für "ganzzahlige Werte überprüfter IP-Adres-

sen", d.h. $\frac{k}{l} \in \mathbb{N}$, durch Erweiterung der Funktion $F(k)$ (4.2) zu:

$$G(k,l) := 1 - \left(1 - \left(P(A) \cdot \sum_{i=1}^{l} P(B_i)\right)\right)^{\frac{k}{l}} \tag{4.5}$$

Der Exponent $\frac{k}{l}$ ist dadurch bedingt, dass bei gleicher Versuchsanzahl k weniger IP-Adressen überprüft werden können, wenn mehr Ports überprüft werden.

Die Funktion $G(k,l)$ wurde für ganzzahlige Werte von $\frac{k}{l}$ definiert. Für die "Zwischenschritte" ist die Port-Verteilung zu berücksichtigen. Hierzu wird zunächst $G(k,l)$ wie folgt umgeformt:

$$G(k,l) = 1 - \left(1 - \left(P(A) \cdot \sum_{i=1}^{l} P(B_i)\right)\right)^{\frac{k}{l}-1} \cdot \left(P(A) \cdot \sum_{i=0}^{l} P(B_i)\right)$$

Berücksichtigt man beim letzten Term die Port-Verteilung ergibt sich:

$$G^*(k,l) := 1 - \left(1 - \left(P(A) \cdot \sum_{i=1}^{l} P(B_i)\right)\right)^{\lfloor \frac{k}{l} \rfloor} \cdot \left(P(A) \cdot \sum_{i=1}^{k \bmod l} P(B_i)\right)$$

Zur Illustration zeigt Abb. 4.15 eine exemplarische Berechnung mit den Port-Wahrscheinlichkeiten $P(B_1) = 0,4; P(B_2) = 0,4; P(B_3) = 0,2$ und $P(A) = 0,2$. Die Linien wurden dabei mittels $G^*(k,l)$ berechnet und die Punkte durch eine Simulation des entsprechenden Szenarios bestimmt. Dass es effizienter oder weniger effizient sein kann mehrere Ports einer IP-Adresse zu überprüfen, zeigt die genannte Port-Verteilung exemplarisch. So ist die Wahrscheinlichkeit einen Knoten nach k Versuchen zu finden in dem Beispiel bei zwei Ports am größten, wie Abb. 4.15 zeigt. Insofern stellt sich die Frage nach dem Optimum.

Da die Wahrscheinlichkeit $P(A)$ in der Regel jedoch gering ist, kann die Formulierung des Optimierungsproblems durch $G(k,l)$ erfolgen. Dann ergibt sich die optimale Suchstrategie durch:

$$\begin{aligned}
&\max\{G(k,l)\} \Leftrightarrow \\
&\max\left\{1 - \left(1 - \left(P(A) \cdot \sum_{i=1}^{l} P(B_i)\right)\right)^{\frac{k}{l}}\right\} \Leftrightarrow \\
&\min\left\{\left(1 - \left(P(A) \cdot \sum_{i=1}^{l} P(B_i)\right)\right)^{\frac{k}{l}}\right\} \Leftrightarrow
\end{aligned}$$

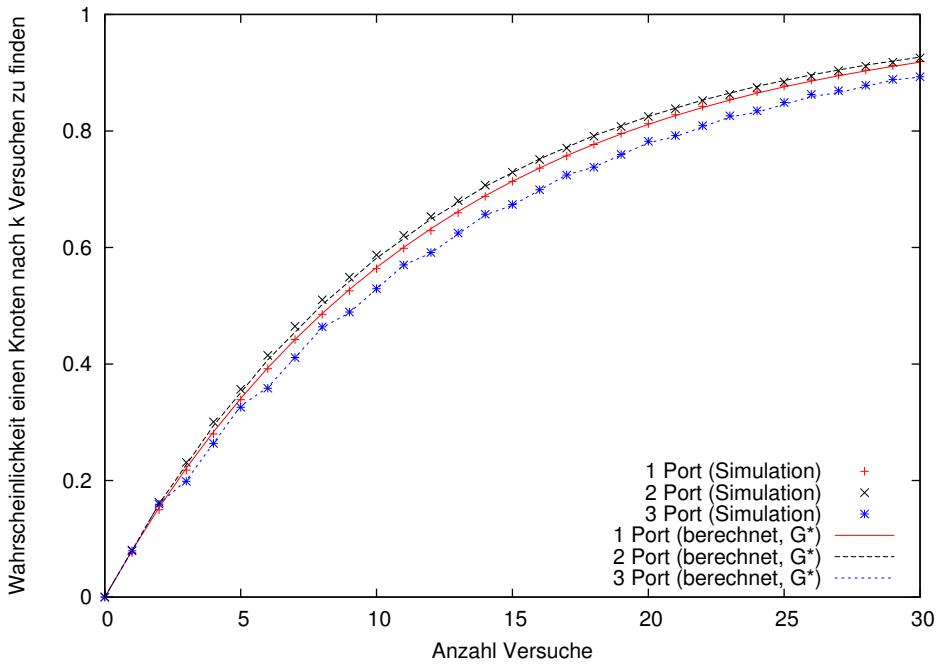


Abbildung 4.15: Berechnete Wahrscheinlichkeiten durch $G^*(k, l)$ im Vergleich zu Simulationsergebnissen mit exemplarischer Port-Verteilung

$$\min \left\{ \sqrt[l]{\left(1 - \left(P(A) \cdot \sum_{i=1}^{l} P(B_i)\right)\right)} \right\} \tag{4.6}$$

Bei bekannter Port-Verteilung kann somit die optimale Anzahl der zu überprüfenden Ports durch Iteration über alle möglichen l bestimmt werden. Da $l \leqslant b$ gilt und bei UDP maximal $b = 65.536$ mögliche Ports zu überprüfen sind, stellt die Lösung des Optimierungsproblems (4.6) durch Iteration über alle möglichen l für aktuelle Rechner kein Problem dar, da die Berechnung nur wenige Sekunden benötigt.

4.2.6 Nachweis des Optimums bei gleichverteilten Ports

Mittels des Terms (4.6) kann das Optimum für eine beliebige Port-Verteilung bestimmt werden, d.h. die optimale Zahl zu überprüfender Ports ermittelt werden. Sind die genutzten Ports jedoch gleichverteilt, stellt sich die Frage nach einer generellen Strategie. In der BitTorrent-DHT sind die Ports zurzeit zwar nicht gleichverteilt wie Abb. 4.11 zeigt. Zukünftig kann es allerdings zu einer solchen Gleichverteilung kommen, da die Ports durch aktuelle P2P-Anwendungen zufällig gewählt werden (vgl. Abschnitt 4.2.4). Eine Gleichverteilung muss dabei nicht bedeuten, dass alle 65.536 möglichen Ports gleichmäßig genutzt werden. So handelt

es sich auch um eine Gleichverteilung, wenn immer ein Port zwischen 1024 und 32.000 zufällig gewählt wird.

Insofern wird im Folgenden untersucht, welche Suchstrategie bei einer angenommen Gleichverteilung der Ports am effizientesten ist. Dabei wird durch einen analytischen Nachweis gezeigt, dass es im Falle einer Gleichverteilung in jedem Falle gewinnbringender ist, alle Ports zu überprüfen.

Voraussetzung und Nebenbedingungen: Wie zuvor werden folgende Voraussetzungen angenommen:

- $P(A)$ entspricht der Wahrscheinlichkeit, dass unter einer zufällig gewählten IP-Adresse ein Knoten betrieben wird.
- $P(B_i)$ entspricht der Wahrscheinlichkeit, dass ein Knoten den Port i nutzt.
- O.b.d.A. gelte: $P(B_i) \geqslant P(B_j)$ für $1 \leqslant i < j \leqslant b$.
- $\exists\, l_0 \in \mathbb{N} : \sum_{i=1}^{l_0} P(B_i) = 1$ und für $i > l_0$ gilt daher $P(B_i) = 0$.
- O.b.d.A. gelte für l daher: $1 \leqslant l \leqslant l_0 \leqslant b$.
- Weiterhin gilt: $0 \leqslant P(A) \cdot \sum_{i=1}^{l} P(B_i) \leqslant 1$.

Für den Fall der Gleichverteilung folgt somit:

$$P(B_i) = P(B_j) = \frac{1}{l_0} \text{ für } 1 \leqslant i, j \leqslant l_0$$

Weiterhin soll c wie folgt definiert werden:

$$c := P(A) \cdot P(B_i) = P(A) \cdot \frac{1}{l_0}$$

Dann gilt: $0 \leqslant c \leqslant 1$ sowie $0 \leqslant c \cdot l \leqslant 1$ mit $1 \leqslant l \leqslant l_0$ und es folgt: $c \leqslant \frac{1}{l_0}$.

Optimierungsproblem bei gleichverteilten Ports: Unter den genannten Voraussetzungen kann das Optimierungsproblem entsprechend dem Term (4.6) bei gleichverteilten Ports folgendermaßen umformuliert werden:

$$\max \left\{ 1 - \sqrt[l]{\left(1 - (P(A) \cdot \sum_{i=1}^{l} P(B_i)) \right)} \right\} \Leftrightarrow$$

$$\min \left\{ \left(1 - (P(A) \cdot \sum_{i=1}^{l} P(B_i)) \right)^{\frac{1}{l}} \right\} \Leftrightarrow$$

$$\min \left\{ (1 - P(A) \cdot l \cdot P(B_i))^{\frac{1}{l}} \right\} \Leftrightarrow$$

$$\min\left\{(1-(c\cdot l))^{\frac{1}{l}}\right\} \tag{4.7}$$

Es stellt sich nun die Frage, ob eine allgemeine Aussage, die unabhängig von den Wahrscheinlichkeiten $P(A)$ und $P(B_i)$ ist, für gleichverteilte Ports getroffen werden kann. Anders formuliert, ist es effizienter zunächst alle Ports einer IP-Adresse zu untersuchen oder immer eine andere IP-Adresse zu nutzen?

Im Folgenden wird gezeigt, dass es effizienter ist alle Ports einer IP-Adresse zu durchsuchen. Übertragen auf das Optimierungsproblem (4.7) und einer gleichen Anzahl von Versuchen bleibt daher folgendes Theorem zu zeigen.

Theorem: Es gilt unter den genannten Voraussetzungen und Nebenbedingungen:

$$(1-(c\cdot l))^{\frac{1}{l}} \geqslant (1-(c\cdot l+1))^{\frac{1}{l+1}} \tag{4.8}$$

Beweis: Für $l = 1$ kann der Beweis wie folgt erbracht werden:

$$\begin{aligned}
(1-cl)^{\frac{1}{l}} &\geqslant (1-c(l+1))^{\frac{1}{l+1}} \\
(1-c) &> (1-2c)^{\frac{1}{2}} \\
1 &\geqslant \frac{\sqrt{1-2c}}{1-c} = \sqrt{\frac{1-2c+c^2-c^2}{(1-c)^2}} \\
1 &\geqslant \sqrt{1-\left(\frac{c}{1-c}\right)^2}
\end{aligned}$$

Ein Fortführung mittels vollständiger Induktion gelang jedoch nicht, so dass eine alternative Methode des Nachweises gewählt wurde.

Die Kernidee des Beweises besteht darin die folgende Funktion $f(l,c)$ zu definieren und zu zeigen, dass diese monoton fallend ist. Abb. 4.16 zeigt die Funktion hierzu für exemplarische Werte von c und l[11].

$$f(l,c) := (1-cl)^{\frac{1}{l}} \text{ für } D_f = ([1,1/c],[0,1/l])$$

Die Funktion ist stetig und im Definitionsbereich D_f differenzierbar. Zum Zweck des Nachweises soll $f(k,c)$ daher differenziert werden. Zunächst sei dazu $l = l_f$ fest und die partielle Ableitung $f'(l_f,c)$ ergibt sich zu:

$$f'(l_f,c) = -\frac{(1-cl)^{\frac{1}{l}}}{1-cl}$$

[11] Die Funktion $f(l,c)$ wurde für die Abb. 4.16 aus darstellungstechnischen Gründen erweitert, so dass $f(l,c) = 0$ für $c > \frac{1}{l},\ c \geqslant 0,\ l \geqslant 1$ gilt.

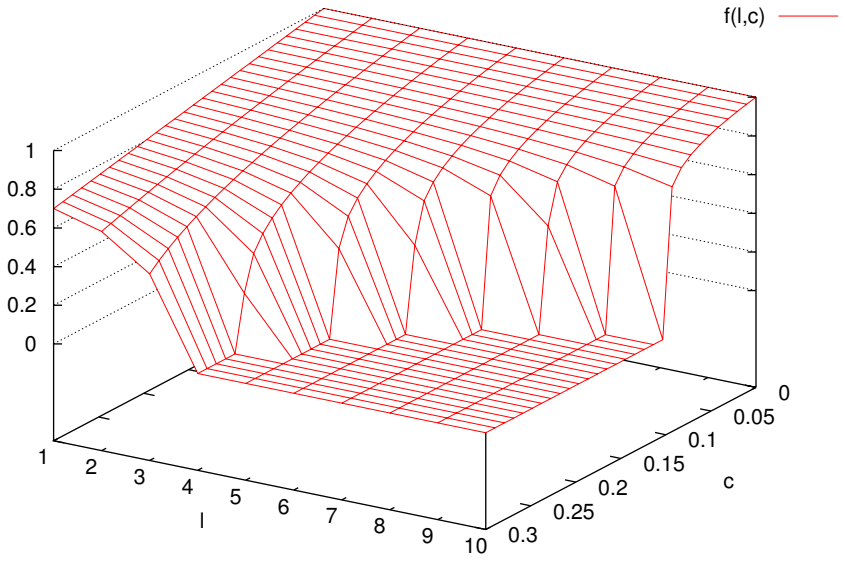


Abbildung 4.16: Exemplarische Darstellung der Funktion *f(l,c)*

Für den fraglichen Bereich D_f gilt $f'(l_f, c) \leqslant 0$, da $0 \leqslant cl \leqslant 1$. Somit ist $f(l_f, c)$ monoton fallend. Jetzt sei $c = c_f$ fest. Ferner sei:

$$f(x) := g(x)^{h(x)} = e^{h(x) \cdot \ln(g(x))}$$

Dann gilt:

$$f'(x) = \left(h'(x) \cdot \ln(g(x)) + h(x) \cdot \frac{g'(x)}{g(x)} \right) \cdot g(x)^{h(x)}$$

Somit folgt für die Funktion $f(l, c_f)$ und die partielle Ableitung $f'(l, c_f)$:

$$\begin{aligned} f(l, c_f) &= (1 - cl)^{\frac{1}{l}} \\ g(l, c_f) &:= 1 - cl \\ h(l, c_f) &:= \frac{1}{l} \\ g'(l) &= -c \\ h'(l) &= -\frac{1}{l^2} \end{aligned}$$

$$\begin{aligned} f'(l, c_f) &= \left(-\frac{1}{l^2} \cdot \ln(1 - cl) + \frac{1}{l} \cdot \frac{-c}{1 - cl} \right) \cdot (1 - cl)^{\frac{1}{l}} \\ &= (1 - cl)^{\frac{1}{l}} \cdot \left(-\frac{\ln(1 - cl)}{l^2} - \frac{c}{l(1 - cl)} \right) \end{aligned}$$

Zu zeigen bleibt, dass $f'(l, c_f) \leqslant 0$ ist. Dabei gilt $(1 - cl)^{\frac{1}{l}} \geqslant 0$ für $0 \leqslant cl \leqslant 1$.

Insofern bleibt zu beweisen, dass die folgende Ungleichung (4.9) unter der Einschränkung $0 \leqslant cl \leqslant 1$ gilt.

$$0 \geqslant -\left(\frac{\ln(1-cl)}{l^2} + \frac{c}{l(1-cl)}\right) \Leftrightarrow \tag{4.9}$$

$$\begin{aligned} 0 &\leqslant \left(\frac{\ln(1-cl)}{l^2} + \frac{c}{l(1-cl)}\right) \Leftrightarrow \\ 0 &\leqslant \left(\frac{\ln(1-cl)\cdot(1-cl)+cl}{l\cdot(1-cl)}\right) \Leftrightarrow \\ 0 &\leqslant \ln(1-cl)\cdot(1-cl)+cl \end{aligned}$$

Da die Korrektheit der Ungleichung sich nicht unmittelbar ergibt, soll die Hilfsfunktion $f_1(l,c)$ definiert werden:

$$f_1(l,c) = \ln(1-cl)\cdot(1-cl)+cl$$

Für $l = 1$ und $c = 0$ gilt: $f_1(1,0) = \ln(1)\cdot(1)+0 = 0$ und die partiellen Ableitungen ergeben sich zu:

$$\begin{aligned} f_1'(l_f,c) &= -\ln(1-cl)\cdot c \\ f_1'(l,c_f) &= -\ln(1-cl)\cdot c \end{aligned}$$

Somit folgt für $0 \leqslant 1-cl \leqslant 1$, dass $f_1'(l,c) > 0$ und daher die obige Ungleichung (4.9) erfüllt ist. Weiterhin folgt daraus, dass $f'(l,c_f) \leqslant 0$ ist und damit $f(l,c_f)$ monoton fallend ist.

Aus beiden partiellen Ableitungen folgt somit, dass die Funktion $f(l,c)$ monoton fallend ist und das Theorem (4.8) bewiesen ist.

□

Aus dem Beweis des Theorems (4.8) folgt, dass bei gleichverteilten Ports eine Knotensuche immer zunächst die Ports von 1 bis l_0 durchsucht werden sollten bevor die nächste IP-Adresse untersucht wird. Dabei ist es unerheblich, um wie viele Ports es sich handelt oder wie hoch die Wahrscheinlichkeit $P(A)$ für einen Knoten je IP-Adresse ist. Dabei bleibt jedoch auch zu beachten, dass dieses Ergebnis nur für gleichverteilte Ports gilt und im Falle einer anders gearteten Verteilung das Optimum mittels der Formel (4.6) zu bestimmen ist.

4.2.7 Optimiertes Probing durch filterresistente Port-Selektion

Wie aus den vorigen Abschnitten deutlich wurde, bereitet eine hohe Entropie bei der Port-Verteilung beim Probing erhebliche Probleme, da sich der Suchraum wesentlich vergrößert. Aus Sicht der Entwickler eines P2P-Systems ist die zufällige Port-Wahl aber vorteilhaft, da es so Internet Service Providern (ISP) nicht mehr möglich ist, den Datenverkehr eines bestimmten P2P-Systems anhand des Ports zu filtern.

Im Folgenden wird daher ein Verfahren zur gezielten Port-Selektion vorgeschlagen, dass keine einfache Port-Filterung zulässt und gleichzeitig den Aufwand des Probing deutlich reduziert. Dieses Verfahren macht sich zunutze, dass die Ressourcen zur Filterung von Datenverkehr bei ISPs, genauer in den Routern, begrenzt sind. Limitierende Komponente eines Routers ist dabei der so genannte Ternary Content Addressable Memory (TCAM) [Lakshminarayanan et al. 2005], durch welchen die Access Control Lists (ACLs) realisiert werden (vgl. auch [Dinger & Hartenstein 2008, S. 35]). Aufgrund der beschränkten Größe eines TCAMs ist es in der Regel nicht möglich, für jede IP-Adresse dedizierte Filterregeln zu definieren. Vielmehr werden Filterregeln für IP-Adressbereiche festgelegt. Die gezielte Selektion eines Ports kann daher folgendermaßen erfolgen[12]:

> Auf Basis der IP-Adresse $\mathtt{ipAddr}$ eines Knotens und einem "virtuellen Standard-Port" $\mathtt{port}_{\mathtt{virt}}$ kann der tatsächliche Port $\mathtt{port}_{\mathtt{real}}$ berechnet werden durch:
>
> $$\mathtt{port}_{\mathtt{real}} := \mathtt{h}(\ \mathtt{ipAddr} \otimes \mathtt{port}_{\mathtt{virt}}\ ) \bmod 2^{16}$$
>
> Dabei entspricht $\mathtt{h}(x)$ einer konsistenten Hash-Funktion wie zum Beispiel SHA-1 [FIP 180-2] und der virtuelle Standard-Port $\mathtt{port}_{\mathtt{virt}}$ einem beliebigen, aber fixierten Port.

Mittels dieser gezielten Port-Selektion sind die resultierenden Ports $\mathtt{port}_{\mathtt{real}}$ über dem möglichen Port-Raum einerseits gleichverteilt, so dass eine einfache Port-Filterung nicht möglich ist. Beim Probing kann der potentielle Port $\mathtt{port}_{\mathtt{real}}$ jedoch sehr leicht errechnet werden, da die untersuchte IP-Adresse $\mathtt{ipAddr}$ und der virtuelle Standard-Port $\mathtt{port}_{\mathtt{virt}}$ bekannt sind.

Vorteilhaft bei diesem Verfahren ist außerdem die Tatsache, dass nicht alle Peers eines P2P-System das Verfahren anwenden müssen und insofern eine langsame Migration erfolgen kann.

[12] Aus Gründen der besseren Lesbarkeit wurden an dieser Stelle mehrere Zeichen zur Auszeichnung der Elemente verwendet.

4.2.8 Resümee

Kern der dargelegten kollaborativen P2P-Architektur ist die Nutzung eines weit verbreiteten P2P-Systems für das Bootstrapping von kleinen, so genannten Mikro-P2P-Systemen. Die empirische Studie innerhalb der BitTorrent-DHT zeigt, dass solch ein Verfahren tragfähig ist. So wurde bei einer Suchrate von 100 pkt/s in Zugangsnetzen mit einer Wahrscheinlichkeit von 95 % nach 12 Minuten mindestens ein Knoten gefunden. Dabei erweist sich vor allem die Suche in Zugangsnetzen als zielführend, da die Knotendichte dort höher ist. Ferner beschleunigt ein lokaler Host Cache den Vorgang wesentlich, da ein kleiner Teil der Knoten sehr lange in der BitTorrent-DHT unter der gleichen Adresse erreichbar ist und letztlich ein einziger noch aktiver Knoten im Host Cache ausreicht, um erfolgreich der DHT beizutreten. Dies konnte durch Messung der Sitzungsdauer von BitTorrent-DHT-Knoten gezeigt werden.

Die zufällige Adressprüfung wird mittlerweile erschwert, da die UDP-Ports zufällig gewählt werden und der Suchraum somit im ungünstigsten Fall um 2^{16} vergrößert wird. Dies konnte durch Analyse der Port-Verteilung bestätigt werden, die zeigt dass lediglich 1,3 % der Knoten den vormaligen Standard-Port nutzen.

Durch das analytisch formulierte Optimierungsproblem kann eine Bewertung und letztlich auch Optimierung der Suche für beliebige Port-Verteilungen durchgeführt werden. Weiterhin wurde nachgewiesen, dass bei einer Gleichverteilung der Ports, die optimale Strategie immer darin besteht zunächst alle potentiellen Ports zu durchsuchen und dann erst zur nächsten IP-Adresse zu wechseln.

Um die Suche in zukünftigen P2P-Systemen zu beschleunigen, wurde ein Verfahren zum optimierten Probing durch filterresistente Port-Selektion entworfen. Bei diesem Verfahren verwenden die Knoten auch unterschiedliche Ports. Die Ports können jedoch auf Basis der IP-Adresse mittels einer Hash-Funktion berechnet werden. Dadurch ist pro IP-Adresse wieder nur ein Port zu prüfen ist und die Suche wird erheblich beschleunigt, da sich der Suchraum verringert.

4.3 Zusammenfassung

Ziel dieses Kapitels war es, das mögliche Potential von P2P-Systemen hinsichtlich komplexer Anwendungsszenarien sowie geringer Teilnehmerzahlen zu analysieren.

Durch die entwickelte dienstorientierte P2P-Architektur konnte gezeigt werden, wie sich P2P-Techniken in komplexe verteilte Systeme wie einen “dezentralen elektronischen Marktplatz” integrieren und gewinnbringend nutzen lassen. Das Einsatzspektrum von P2P-Systemen wurde durch die dargelegte Architektur

wesentlich erweitert, indem Web Services-Technologien mit P2P-Netzen kombiniert wurden.

Da vor allem der Beitritt bzw. Aufbau eines Mikro-P2P-Systems mit wenigen Teilnehmern problembehaftet ist, wurde mittels der kollaborativen P2P-Architektur eine Möglichkeit geschaffen durch die (Mit-)Nutzung eines weit verbreiteten P2P-Systems ein solches System vollständig dezentral zu realisieren. Durch eine empirische Studie in der BitTorrent-DHT konnte gezeigt werden, dass ein Beitritt zu dem weit verbreiteten P2P-System mittels einer zufälligen Adressprüfung (engl. Probing) innerhalb weniger Minuten möglich ist. Weiterhin konnte die Suchdauer mittels der analytischen Formulierung eines Optimierungsproblems für beliebige P2P-Systeme optimiert werden. Abschließend wurde das neuartige Verfahren "Optimiertes Probing durch filterresistente Port-Selektion" erläutert, durch welches die Suche in zukünftigen P2P-Systemen wesentlich beschleunigt wird.

Insgesamt konnten durch das Kapitel einerseits die Grenzen bestehender P2P-Systeme aufgezeigt werden. Andererseits wurde das Einsatzspektrum durch die entwickelten Architekturen deutlich erweitert.

5

Sybil-Angriff: ressourcenbasierte Analyse und Selbstregistrierung

Ziel dieses Kapitels ist es, den Aspekt Robustheit in P2P-Systemen und -Netzen differenziert zu untersuchen. Nach einer Betrachtung zur Fehlertoleranz werden P2P-spezifische Angriffe sowie die daraus resultierenden Gefahren aufgezeigt.

Dabei erweist sich der Sybil-Angriff, bei dem ein Angreifer versucht, unter mehreren Identitäten im P2P-Netz zu agieren, als besonders schwerwiegend. Für den Betrieb dieser zusätzlichen Knoten benötigt ein Angreifer Ressourcen. Bislang finden sich jedoch keine adäquaten Abschätzungen darüber, mit welchen Ressourcen welcher Einfluss ausgeübt werden kann. Insofern wird in dieser Arbeit mittels einer ressourcenbasierte Analyse bestimmt, wie viele Netzbandbreite, Rechenleistung und Speicher für den Betrieb eines Knotens nötig sind. Die Analyse basiert auf Daten, die durch umfangreiche Messungen in realweltlichen P2P-Systemen im Internet gewonnen wurden. Darüber hinaus wird durch nachgelagerte simulative Studien gezeigt, wie sich diese Ressourcen zur Limitierung des Einflusses eines Angreifers nutzen lassen.

Ein Angreifer verfügt in der Regel auch nur über eine beschränkte Anzahl von IP-Adressen, wobei bislang fraglich blieb wie sich diese Limitierung effektiv zur Beschränkung eines Sybil-Angriffs nutzen lässt. Durch die Entwicklung eines neuartigen Selbstregistrierungsverfahrens gelingt es letztlich die Anzahl der Knoten pro IP-Adresse bzw. IP-Adressbereich zu begrenzen. Insgesamt kann so-

mit der Einfluss, den ein Angreifer erlangen kann, deutlich eingeschränkt bzw. die erforderlichen Ressourcen deutlich erhöht werden.

Es findet bewusst keine Spezifikation eines konkreten Anwendungsszenarios und insbesondere keine Festlegung der anzunehmenden Knotenanzahl statt, da diese, wie das vorige Kapitel zeigt, sehr unterschiedlich sein kann. Vielmehr sollen Entwickler und Betreiber die dargelegten Bewertungsmethoden und diskutierten Abwägungsentscheidung nutzen, um das Gefahrenpotential von P2P-Systemen in konkreten Kontexten beurteilen zu können.

5.1 Abgrenzung von Robustheit und Fehlertoleranz in P2P-Systemen

Nach der Definition des *IEEE Standard Computer Dictionary* [IEEE 1991] versteht man unter Robustheit den Grad, zu welchem ein System oder eine Komponente in der Gegenwart falscher Eingaben oder schwieriger Umgebungsbedingungen noch korrekt funktioniert.

> *"Robustness. The degree to which a system or component can function correctly in the presence of invalid inputs or stressful environmental conditions. See also: error tolerance; fault tolerance."*
> aus [IEEE 1991, S. 174]

Vorrangiges Ziel eines P2P-Systems ist es, Ressourcen gegenseitig zu nutzen (vgl. Abschnitt 2.3). Als korrekte Funktion des Systems kann insofern die Eigenschaft angesehen werden, dass die gesuchten Ressourcen zugänglich sind. Um die Robustheit von P2P-Systemen unter Berücksichtigung der vorgenannten Begriffsdefinition zu beurteilen, sind somit fehlerhafte Eingaben und das fehlerhafte Verhalten einzelner Knoten ebenso zu berücksichtigen wie gezielte Angriffe durch mehrere Knoten[1], die die korrekte Funktion des Systems beeinflussen. Von Nutzern unabsichtlich herbeigeführte Fehler können darunter subsumiert werden, da der maximale Schaden nicht größer sein kann als der Schaden, der durch den effizientesten Angriff entsteht.

> *"fault tolerance. (1) The ability of a system or component to continue normal operation despite the presence of hardware or software faults. See also: error tolerance; fail safe; fail soft; fault secure; robustness. (2) The number of faults a system or component can withstand before normal operation is impaired.*

[1] in diesem Sinne auch [Androutsellis-Theotokis & Spinellis 2004, S. 349, 359]

> *(3) Pertaining to the study of errors, faults, and failures, and of methods for enabling systems to continue normal operation in the presence of faults. See also: recovery (2); redundancy; restart.*"
> aus [IEEE 1991, S. 87]

Bei der Beurteilung der Robustheit eines Systems ist auch dessen Fehlertoleranz zu berücksichtigen. Die Fehlertoleranz ist gemäß *IEEE Standard Computer Dictionary* wie folgt definiert: i) Fehlertoleranz ist die Fähigkeit eines Systems oder einer Komponente trotz des Auftretens von Hard- oder Software-Fehlern den normalen Betrieb fortzusetzen. ii) Die Anzahl der Fehler, der ein System oder eine Komponente widerstehen kann, bis der normale Betrieb beeinträchtigt ist, wird auch als Fehlertoleranz bezeichnet. iii) Untersuchungen betreffend Fehlfunktionen[2] und Methoden, die es Systemen ermöglichen trotz der Präsenz von Fehlern ihren normalen Betrieb fortzusetzen, werden auch unter dem Begriff Fehlertoleranz gefasst.

Die Differenzierung der beiden Begrifflichkeiten Robustheit und Fehlertoleranz soll im weiteren Verlauf der Arbeit anhand folgender Merkmale erfolgen: Bei der Robustheit sind *äußere Einflüsse* wie fehlerhafte Eingaben, Änderungen der Umgebung und somit insbesondere auch gezielte Angriffe von Belang. Im Gegensatz dazu beschreibt Fehlertoleranz die *inhärente Fähigkeit* eines Systems, trotz des Ausfalls bzw. Fehlverhaltens einzelner Teile des Systems den Betrieb korrekt fortzusetzen.

Die Bewertung der Fehlertoleranz erfolgt somit als "innere Betrachtung" und insofern werden Annahmen über das System, wie zum Beispiel den Anteil ausfallender Komponenten, gemacht. Bei der Robustheitsbetrachtung wird hingegen der Kontext, in dem das System betrieben wird, mit einbezogen.

Eine strikte Trennung von innerer und äußerer Betrachtung fällt bei P2P-Systemen schwer, da es sich um offene Systeme handelt. Dennoch ist einen Separation dienlich, um eine Kategorisierung der zu untersuchenden Aspekte vorzunehmen. Dies spiegelt sich insofern in den weiteren Abschnitten wider.

P2P-Systeme gelten aufgrund der immanenten Dezentralität in Verbindung mit der redundanten Speicherung von Daten und alternativen, redundanten Routen im Overlay-Netz als sehr fehlertolerant (vgl. u.a. [Milojicic et al. 2002, S. 12]). Dennoch lassen viele Autoren häufig die entsprechenden wahrscheinlichkeitstheoretischen Betrachtungen außer Acht, die letztlich einen teilweise immensen Bedarf an Redundanz aufzeigen. Insofern wird im Folgenden zunächst die Fehlertoleranz in P2P-Netzen vertieft diskutiert.

[2] Für die Differenzierung von Error, Fault und Failure sei auf [IEEE 1991] verwiesen, wobei die definierten Unterschiede für die weiteren Betrachtungen in dieser Arbeit unerheblich sind.

Fraglich bleibt weiterhin, inwiefern diese Redundanz durch Angriffe unterminiert werden kann. Daher erfolgt darauf aufbauend die Darlegung P2P-spezifischer Angriffe und letztlich die Fokussierung auf den Sybil-Angriff.

Bei den folgenden Ausführungen bleibt zu berücksichtigen, dass eine exakte Bestimmung des Robustheitsgrades die Spezifikation eines konkreten Systems sowie der Umgebungsbedingungen erfordert. Insofern findet die Diskussion auf zwei Ebenen statt. Zum einen wird soweit möglich eine Bewertung auf Basis abstrahierter P2P-Systeme bzw. -Netze vorgenommen. Zum anderen werden ausgewählte Aspekte, vor allem konkrete Abwehrmechanismen, anhand des P2P-Netzes Kademlia und der BitTorrent-DHT aufgezeigt.

Ferner bleibt zu berücksichtigen, dass die folgenden Betrachtungen zur Robustheit und Fehlertoleranz P2P-spezifische Aspekte fokussieren. Weitere Fehler und Angriffe, wie sie bspw. durch Pufferüberläufe (engl. Buffer Overflow) entstehen, sind zwar auch bei P2P-Systemen möglich, bleiben jedoch unberücksichtigt.

5.2 Fehlertoleranz durch Redundanz

Bevor eine Bewertung der Fehlertoleranz von P2P-Systemen erfolgt, werden zunächst Grundlagen in Form einer Klassifikation von Fehlerarten sowie einer allgemeinen Betrachtung zu Verfügbarkeit, Mehrheitsentscheidung und dem Konsensusproblem vorgenommen. Anschließend erfolgt die Bewertung der Fehlertoleranz in P2P-Systemen hinsichtlich Datenhaltung und Routing.

5.2.1 Grundlagen

Fehlerklassen: Im Allgemeinen können folgende Fehler unterschieden werden, wobei ein aus Komponenten[3] bestehendes System zugrunde gelegt wird [Barborak et al. 1993, S. 182 f]:

- *Fail-Stop-Fehler:* Ein Fail-Stop-Fehler einer Komponente liegt vor, wenn diese nicht mehr reagiert ("gestorben" ist) [Schlichting & Schneider 1983, S. 223]. Bei einem Fail-Stop-Fehler werden von der fehlerhaften Komponente keine, insbesondere keine fehlerhaften Daten ausgesendet. Diese Fehlerart wird daher auch als Fail-Silent bezeichnet. Ferner werden die anderen Komponenten des Systems über das Auftreten des Fehlers informiert bzw. können den Fehler ohne Weiteres feststellen[4].
- *Crash-Fehler:* Der Unterschied zwischen Fail-Stop-Fehlern und Crash-Fehlern besteht darin, dass der Ausfall der fraglichen Komponente von anderen

[3] Statt von Komponenten wird häufig auch von Prozessen oder Prozessoren gesprochen.
[4] Der Fail-Stop-Fehler wird teilweise als Crash-Fehler aufgefasst (vgl. [Bracha & Toueg 1985]).

nicht ohne Weiteres erfasst werden kann. Die anderen Komponenten können den Fehler nur aufgrund ausbleibender Nachrichten und festgelegten Zeitüberschreitungen feststellen.

- *Omission-Fehler:* Werden von einer Komponente einzelne Eingaben nicht verarbeitet, da zum Beispiel Nachrichten auf dem Kommunikationskanal verloren gingen, spricht man von einem Omission-Fehler.
- *Timing-Fehler:* Dieser Fehler tritt auf, wenn eine Komponente eine Aufgabe nicht in der spezifizierten Zeitspanne erledigt. Er wird daher teilweise auch als Performance-Fehler bezeichnet.
- *Incorrect-Computation-Fehler:* Berechnet eine Komponente auf Basis korrekter Eingabedaten eine falsche Ausgabe, handelt es sich um einen Incorrect-Computation-Fehler.
- *Byzantine-Fehler:* Ein byzantinischer Fehler [Lamport et al. 1982] umfasst alle möglichen Fehler und kann daher als universellste Fehlerart angesehen werden. Dabei können fehlerhafte Komponenten insbesondere auch fehlerhafte Ausgaben erzeugen bzw. Nachrichten versenden. Insofern erfasst diese Klasse auch böswillige Knoten, die absichtlich fehlerhafte Ergebnisse erzeugen.

Die Reihenfolge der Aufzählung stellt eine Ordnung dar, bei welcher der Fail-Stop-Fehler im Crash-Fehler usw. enthalten ist [Barborak et al. 1993, S. 183]. Der Fail-Stop-Fehler ist dabei der einfachste und der Byzantine-Fehler der schwerwiegendste Fehler. Sie dienen daher als Grundlage der weiteren Betrachtungen.

Verfügbarkeit, Mehrheitsentscheidung und Konsensusproblem: Bei der Beurteilung der Fehlertoleranz sind je nach Fehlerart und Anwendungsszenario verschiedene Metriken relevant.

Die *Verfügbarkeit* beim Fail-Stop-Fehlerverhalten entspricht der Wahrscheinlichkeit, dass *eine* von x Komponenten eines komponentenbasierten Systems noch korrekt funktioniert (vgl. auch [IEEE 1991, S. 24]). Insofern wird die Bezeichnung Verfügbarkeit im Folgenden in diesem Sinne verstanden.

Weisen die Komponenten auch byzantinische Fehler auf, ist es nicht nur notwendig, dass eine der möglichen Komponenten korrekt funktioniert. Vielmehr muss in diesem Fall eine *Mehrheitsentscheidung* zwischen den Ergebnissen der einzelnen Komponenten getroffen werden. Insofern müssen für ein korrektes Ergebnis mehr als die Hälfte der Komponenten korrekt sein.

Über einen Mehrheitsentscheid hinaus, befasst sich das *Konsensusproblem* damit, dass alle fehlerfreien Komponenten eines (gegebenenfalls verteilten) Systems trotz des Auftretens von Fehlern zu dem gleichen übereinstimmenden Ergebnis

kommen. In der grundlegenden Arbeit [Lamport et al. 1982] wurde hierfür das so genannte Byzantine Generals Problem formuliert. Dabei ist es das Ziel, dass erstens alle loyalen Generäle einer Armee zu einer gemeinsamen Entscheidung kommen und zweitens die Gruppe der illoyalen, verräterischen Generäle die loyalen nicht von einer anderen Strategie überzeugen können. Die Autoren zeigen, dass die Lösung des Problems (ohne die Nutzung signierter Nachrichten) nur möglich ist, wenn mehr als zwei Drittel der Generäle loyal sind. Weiterhin wird in [Fischer et al. 1985] gezeigt, dass in jedem asynchronen verteilten System bei nur einer Crash-fehlerhaften Komponente eine Möglichkeit existiert, so dass eine Konsensfindung nicht mehr stattfinden kann. Unter der Annahme einer Zeitbeschränkungen für den Abschluss von Prozessen kann jedoch gezeigt werden, dass auch in asynchronen Systemen das Konsensusproblem bei mehr als 2/3 korrekter Komponenten im Falle von byzantinischen Fehlern und bei mehr als der Hälfte korrekter Komponenten im Fall von Crash-Fehlern lösbar ist [Bracha & Toueg 1985]. In der Folge wurden vor allem die Algorithmen zur Lösung des Konsensusproblems optimiert, so dass diese sich effizienter in realen Systemen umsetzen lassen (vgl. u.a. [Castro & Liskov 2002]).

5.2.2 Fehlertoleranz bei P2P-Systemen

Fehler sind bei P2P-Systemen eher die Regel, als die Ausnahme, wie bereits in Abschnitt 2.3.3 ausgeführt wurde. Dennoch kann durch aktive Redundanz[5] ein hoher Grad an Fehlertoleranz erreicht werden [Kubiatowicz 2003, S. 34].

Die folgende Betrachtung differenziert die Datenhaltung bzw. Verfügbarkeit von Ressourcen und das Routing in P2P-Systemen. Abschließend erfolgt eine kombinierte Betrachtung.

Fehlertoleranz bei der Datenhaltung

Um die Verfügbarkeit von Ressourcen in P2P-Systemen zu gewährleisten, werden diese soweit möglich redundant gehalten. Insbesondere bei DHT-basierten Systemen werden die Schlüssel/Wert-Paare mehrfach gespeichert. Im Folgenden wird dargelegt, welche Wahrscheinlichkeiten für die Verfügbarkeit bzw. korrekten Mehrheitsentscheid sich daraus ergeben. Dabei wird die Annahme zugrunde gelegt, dass die Ressourcen direkt erreichbar sind.

Kommt es nur zu Ausfällen von Knoten entsprechend der Fail-Stop-Fehlerklasse, so entspricht die Verfügbarkeit der Wahrscheinlichkeit, dass mindestens

[5] Bei der *aktiven Redundanz* werden Elemente simultan betrieben, um Fehlern zu begegnen. Im Gegensatz zur *Bereitschaftsredundanz* (engl. Standby Redundancy) bei der die redundanten Elemente erst im Fehlerfall zum Einsatz kommen (vgl. u.a. [IEEE 1991]).

einer von r Knoten der für die Datenhaltung zuständig ist noch verfügbar ist. Die Berechnung erfolgt gemäß der Formel (5.1). Dabei entspricht f der Ausfallwahrscheinlichkeit eines Knotens und die Ausfälle seien unabhängig voneinander. Abb. 5.1 zeigt den exemplarischen Verlauf für verschiedene Werte von r.

$$p_{fail} = 1 - f^r \tag{5.1}$$

Nimmt man statt des Fail-Stop-Fehlerverhaltens ein byzantinisches an und führt einen Mehrheitsentscheid durch, ergibt sich die Wahrscheinlichkeit p_{byz} zu:

$$p_{byz} = \sum_{i=\lceil \frac{r+1}{2} \rceil}^{r} \binom{r}{i} f^{r-i}(1-f)^i \tag{5.2}$$

Abb. 5.2 zeigt die Wahrscheinlichkeit für unterschiedliche Werte von r, wobei deutlich wird, dass sich die Wahrscheinlichkeitsverteilung mit zunehmendem r einer Rechtecksverteilung annähert.

Statt einer simplen Replikation kann bei größeren Datenmengen eine Aufspaltung des zu speichernden Datenobjekte in mehrere Blöcke erfolgen (vgl. u.a. [Zhang & Lian 2002; Rodrigues & Liskov 2005]). Die Blöcke werden dann auf unterschiedliche Knoten verteilt und zur Rekonstruktion ist nur ein Teil der Blöcke nötig. Dies als Erasure Coding bezeichnete Verfahren kommt bspw. in dem P2P-System Oceanstore [Kubiatowicz et al. 2000] zur Anwendung. Der Vorteil des Verfahrens besteht insbesondere darin, dass bei gleichem Speicherverbrauch eine wesentlich höhere Verfügbarkeit gegeben ist.

Fehlertoleranz beim Routing

Für das Routing in P2P-Netzen soll im Folgenden eine Abschätzung gegeben werden, anhand derer sich die Fehlertoleranz für unterschiedliche Verfahren bestimmen lässt. Im Gegensatz zur üblichen Differenzierung von P2P-Netzen in strukturierte und unstrukturierte Netze ist an dieser Stelle vielmehr eine Unterscheidung von flutenden Protokollen und nicht-flutenden Protokollen zielführend, wie aus der folgenden Darstellung deutlich wird.

Dabei sei wie zuvor f die Ausfallwahrscheinlichkeit für einen Knoten und die Knotenausfälle unabhängig voneinander. Beim Routing werden wie im vorigen Abschnitt auch Fail-Stop- und byzantinische Fehler unterschieden. Im Falle von Fail-Stop-Fehlern werden eingehende Pakete von dem fehlerhaften Knoten verworfen. Bei byzantinischen Fehlern leitet der fehlerhafte Knoten das Paket hingegen an einen falschen Knoten weiter bzw. liefert eine falsche Antwort.

P2P-Netze sind in der Regel fehlertolerant gegenüber Fail-Stop-Fehlern, da

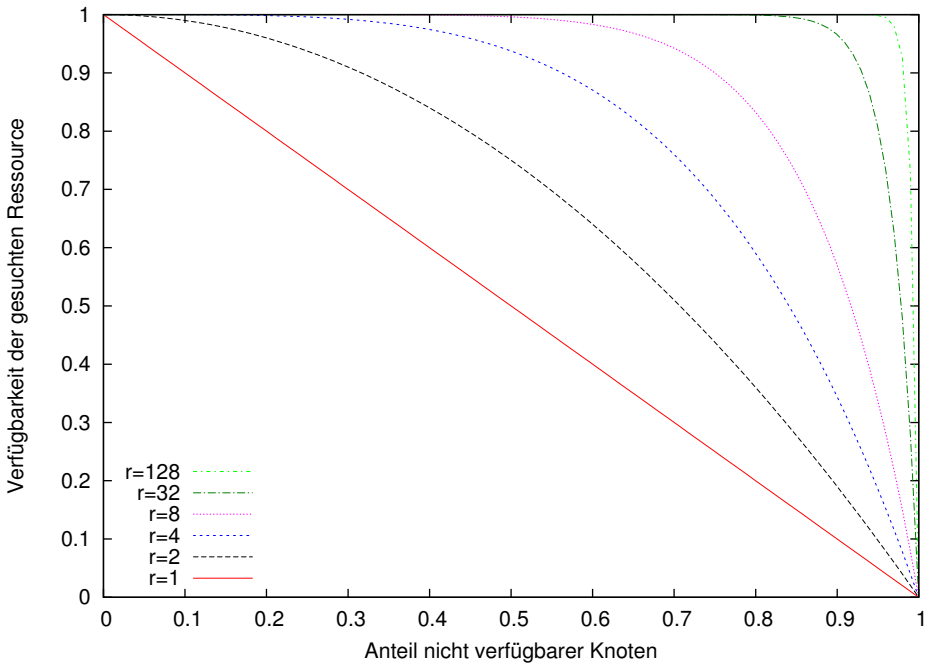


Abbildung 5.1: Verfügbarkeit von Daten bei einer Redundanz von r und Fail-Stop-Fehlerverhalten

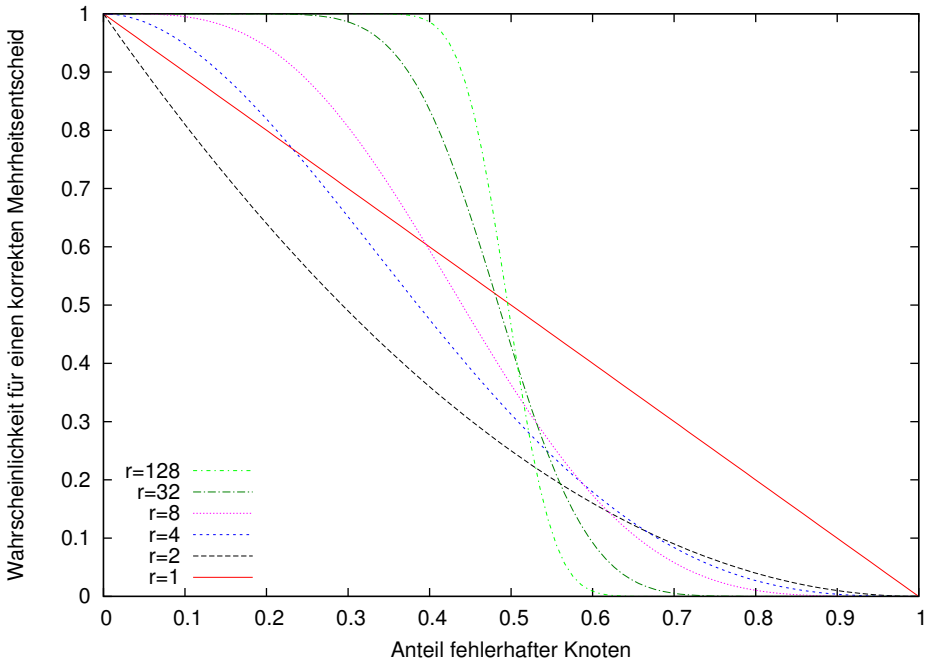


Abbildung 5.2: Wahrscheinlichkeit eines korrekten Mehrheitsentscheids bei einer Redundanz von r und byzantinischem Fehlerverhalten

diese am Ausbleiben einer Antwort erkannt werden können (vgl. u.a. [Rodrigues et al. 2002, S. 118] und [Fiat et al. 2005, S. 805]). Chord kann bspw. bei Nutzung einer Nachfolgerliste mit der Länge $O(\log n)$ bis zu einer Ausfallrate von $f = 0,5$ mit "hoher Wahrscheinlichkeit"[6] noch den korrekten Nachfolgeknoten finden, so dass das Routing korrekt funktioniert [Stoica et al. 2001].

Erreichbarkeit bei flutenden Protokollen: Die Erreichbarkeit von Knoten bei flutenden Protokollen wie Gnutella hängt vor allem vom Vermaschungsgrad des Overlay-Netzes ab. Die beiden Extreme bilden dabei einerseits ein vollvermaschtes Netz und andererseits ein Baum, da im ersten Fall die Anzahl der Verbindungen zwischen den Knoten maximal und im zweiten Falle minimal ist. Die durchschnittliche Erreichbarkeit ergibt sich in beiden Fällen aus dem Quotienten der Anzahl erreichbarer Knoten im Fehlerfall und der Anzahl erreichbarer Knoten im Nicht-Fehlerfall.

Bei einem vollvermaschten Netz entspricht die Erreichbarkeit von Knoten somit der Fehlerwahrscheinlichkeit f derselben, da alle Knoten ohne Zwischenschritte erreichbar sind. Im Falle eines Baumes hängt die Anzahl erreichbarer Knoten von der Anzahl der Kindknoten (im Sinne von Gnutella den Nachbarknoten) sowie der maximalen Hop-Anzahl einer Nachricht ab. Als Vereinfachung wurde für die folgende Betrachtung angenommen, dass die Anzahl Nachbarknoten gleich ist und der betrachtete Knoten die Wurzel des Baumes darstellt. Die Anzahl erreichbarer Knoten ergibt sich somit aus $\sum_{i=1}^{h} m^i$, wobei m der Anzahl Nachbarknoten entspricht und h der maximalen Hop-Anzahl. Die durchschnittliche Anzahl erreichbarer Knoten im Fehlerfall errechnet sich aus $\sum_{i=1}^{h}(m \cdot (1-f))^i$. Somit ergibt sich die durchschnittliche Erreichbarkeit p_{flood} zu der Formel (5.3), wobei sich der zweite Teil aus der geometrischen Reihe ergibt. Durch die Vereinfachung stellt die Formel keine untere Grenze dar, sondern nur eine Annäherung an selbige.

$$p_{flood} = \frac{\sum_{i=1}^{h}(m \cdot (1-f))^i}{\sum_{i=1}^{h} m^i} = \frac{\frac{m(1-f)^{h+1}-1}{m(1-f)-1}}{\frac{m^{h+1}-1}{m-1}} \tag{5.3}$$

Abb. 5.3 zeigt die Erreichbarkeit von Knoten im Verhältnis zur Fehlerrate f für verschiedene Werte von h und m, wobei $h = 7$ für ein Gnutella-Netz typisch ist, wohingegen m typischerweise je nach Knoten unterschiedlich ist. Die Erreichbarkeit im vollvermaschten Netz stellt dabei eine Obergrenze dar. In einem realweltlichen Gnutella-Netzen liegt die Erreichbarkeit zwischen dieser Obergrenze

[6] Nach [Karger et al. 1997, S. 656] meint der Ausdruck "mit hoher Wahrscheinlichkeit" eine Wahrscheinlichkeit von mindestens $1-1/Q$, wobei Q ein Konfidenzparameter darstellt (vgl. auch [Stoica et al. 2001, S. 152]).

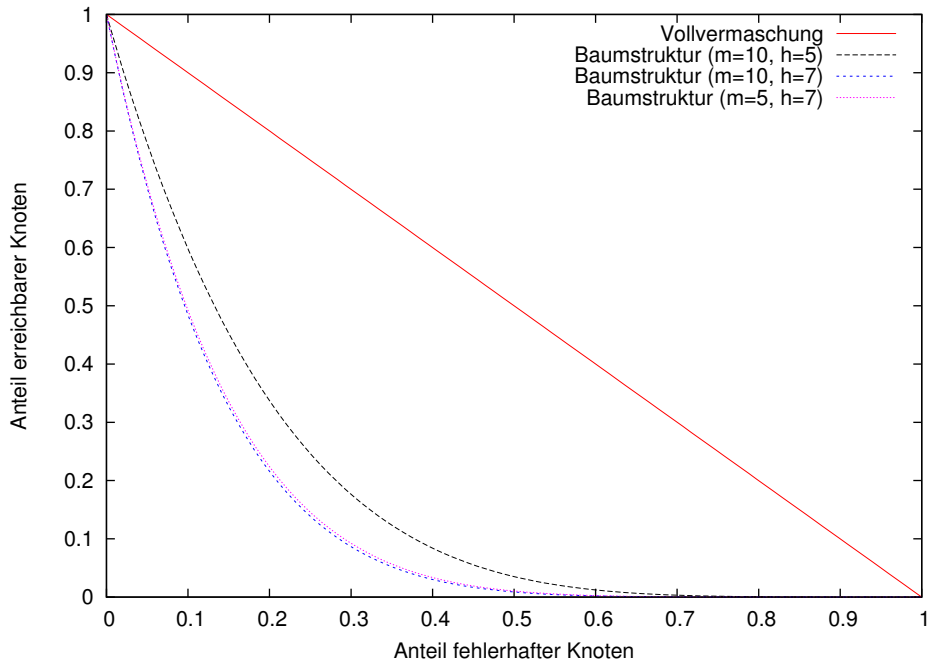


Abbildung 5.3: Erreichbarkeit von Knoten bei flutenden Protokollen

und der vereinfachten Baumstruktur.

Erreichbarkeit bei Pfad-orientierten Protokollen: Bei strukturierten Netzen wie DHTs, aber auch bei Random Walks ergibt sich die durchschnittliche Erreichbarkeit p_{path} aus der Wahrscheinlichkeit, dass alle Knoten des Pfades zum Zielknoten erreichbar sind, so dass für einen Pfad $p_{path} = (1-f)^h$ gilt, wobei h der durchschnittlichen Hop-Anzahl entspricht. Ist es möglich den Zielknoten über d disjunkte Pfade zu erreichen, so gilt die Formel (5.4). Zwei Pfade sind dann disjunkt, wenn kein Knoten (außer Start- und Zielknoten) eines Pfades im anderen Pfad enthalten ist [Castro et al. 2002a].

$$p_{path} = 1-(1-(1-f)^h)^d \tag{5.4}$$

Abb. 5.4 und 5.5 zeigt exemplarisch den Verlauf der Erreichbarkeit des Zielknotens in Abhängigkeit von verschiedenen Werten für d und h. Aus den Abbildungen wird auch deutlich, dass ein zuverlässiges Routing bei nur einem Pfad bereits bei geringen Fehlerraten nur schwerlich möglich ist. Hierzu sei angemerkt, dass in anderen Arbeiten wie [Castro et al. 2002a, Fig. 3] teilweise mit sehr geringen Hop-Anzahl von $h = 2,5$ bis $h = 5$ argumentiert wird. Die Autoren legen dabei das P2P-Netz Pastry zugrunde, bei welchem sich die durchschnittliche Hop-Anzahl aus $h = \log_{2^4}(n)$ ergibt. Bei einer Netzgröße von einer Million Knoten

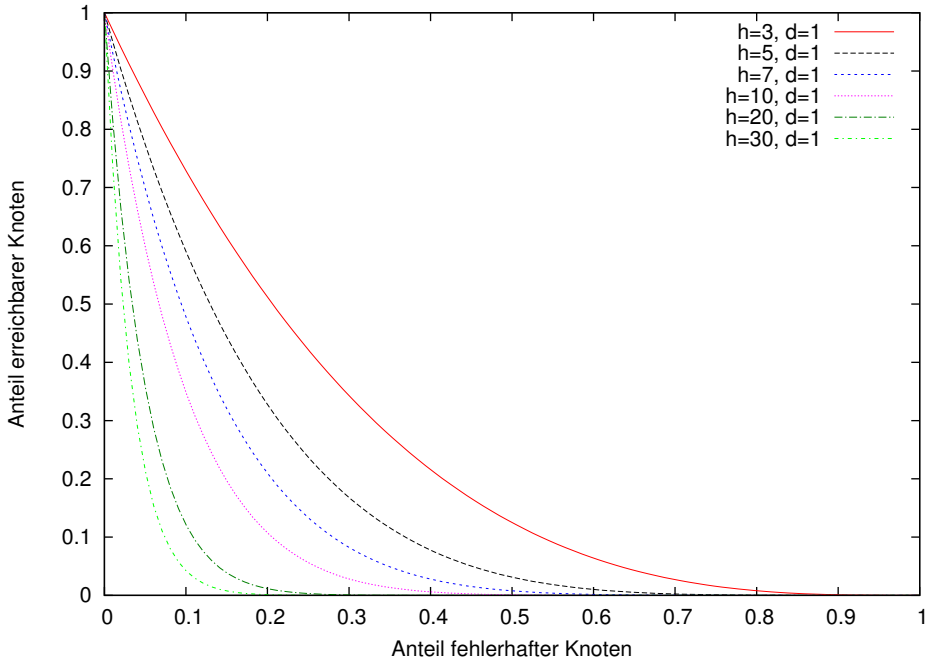


Abbildung 5.4: Erreichbarkeit von Zielknoten bei Pfad-orientierten Protokollen und *einem* Pfad

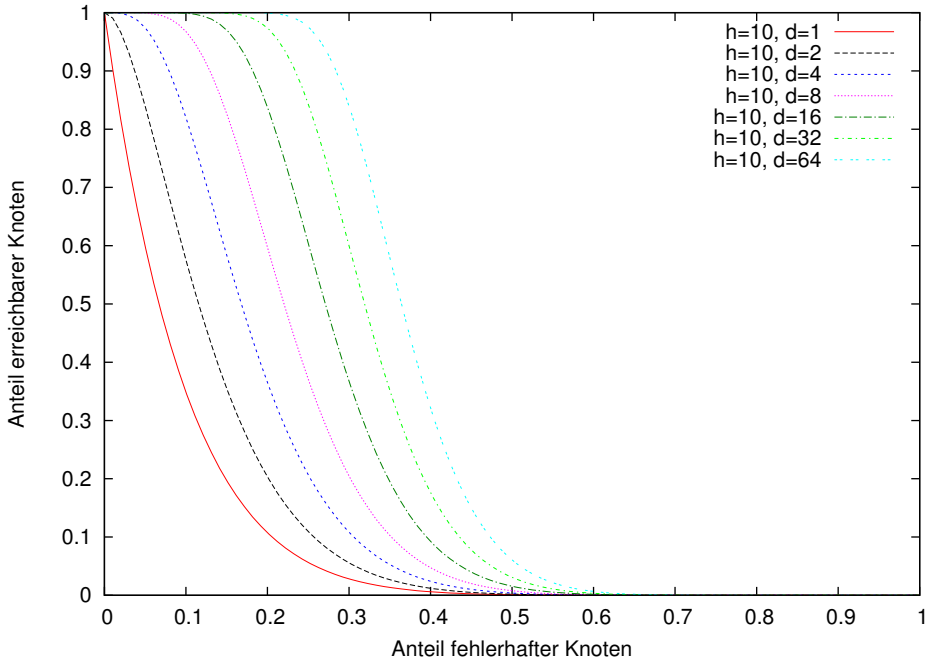


Abbildung 5.5: Erreichbarkeit von Zielknoten bei Pfad-orientierten Protokollen und d disjunkten Pfaden

würde sich bei Kademlia jedoch bereits eine durchschnittliche Hop-Anzahl von $h = 0,5 \cdot \log(n) \approx 10$ ergeben. Messungen in BitTorrent-DHT zeigen gar eine durchschnittliche Hop-Anzahl von mehr als 20 [Crosby & Wallach 2007].

Daher ist die Fehlertoleranz des Routing in P2P-Netzen bei byzantinischem Fehlerverhalten relativ gering bzw. erfordert eine große Anzahl disjunkter Routen.

Beim Routing ist iteratives Routing zu präferieren. Iteratives Routing[7] ist zwar hinsichtlich der Anzahl benötigter Nachrichten als auch Latenz im fehlerfreien Fall weniger effizient als ein rekursives Weiterleiten der Nachrichten. Für die Erkennung von Fehlern, insbesondere Fail-Stop-Fehlern, ist das iterative dem rekursiven Routing jedoch vorzuziehen, da Fehler schneller erkannt werden können und die Kontrolle über das Routing beim initiierenden Knoten verbleibt [Hildrum & Kubiatowicz 2007, S. 322]. Weitere Mechanismen, wie das Routing robuster gegenüber Fehler und gezielten Angriffen gestaltet werden kann, werden in Abschnitt 5.3.3 vorgestellt.

Fehlertoleranz von Routing & Datenhaltung kombiniert

Betrachtet man den erst genannten Punkt der Fehlertoleranz bei der Datenhaltung und das Routing in Kombination, so ist in den Formeln (5.1) und (5.2) die Fehlerwahrscheinlichkeit f durch $1 - p_{flood}$ bzw. $1 - p_{path}$ zu ersetzen. Somit ergibt sich bspw. für eine typische DHT eine durchschnittliche Verfügbarkeit der Einträge bei byzantinischem Fehlerverhalten zu:

$$\sum_{i=\lceil \frac{r+1}{2} \rceil}^{r} \binom{r}{i} (1-(1-f)^h)^{d\cdot(r-i)} (1-(1-(1-f)^h)^d)^i \tag{5.5}$$

Dabei wurde zugrunde gelegt, dass pro Replikation mindestens ein disjunkter Pfad existiert. Abb. 5.6 zeigt beispielhaft welchen Einfluss bereits ein geringer Anteil fehlerhafter Knoten auf eine korrekte Mehrheitsentscheidung hat. Dabei ist auch zu beachten, dass auf der x-Achse nur Werte bis 0,25 aufgetragen sind, um die Vergleichbarkeit zwischen der Abb. 5.6 und 5.7 zu ermöglichen.

Wird statt des byzantinischen Fehlermodells ein Fail-Stop-Modell angenommen, so ergibt sich die Verfügbarkeit aus der Formel (5.1), da das Routing in P2P-Systemen, wie zuvor ausgeführt, tolerant gegenüber Fail-Stop-Fehlern ist.

Zu einer Vermischung der beiden Fehlerarten kann es kommen, falls aufgrund der Dynamik in P2P-Netzen das Routing zum falschen Zielknoten führt, für die

[7] Beim iterativen Routing werden die Datenpakete immer über den initiierende Knoten gesendet, während beim rekursiven Routing eine direkte Weiterleitung von einem Knoten zum anderen stattfindet (vgl. hierzu auch Abschnitt 2.4.3).

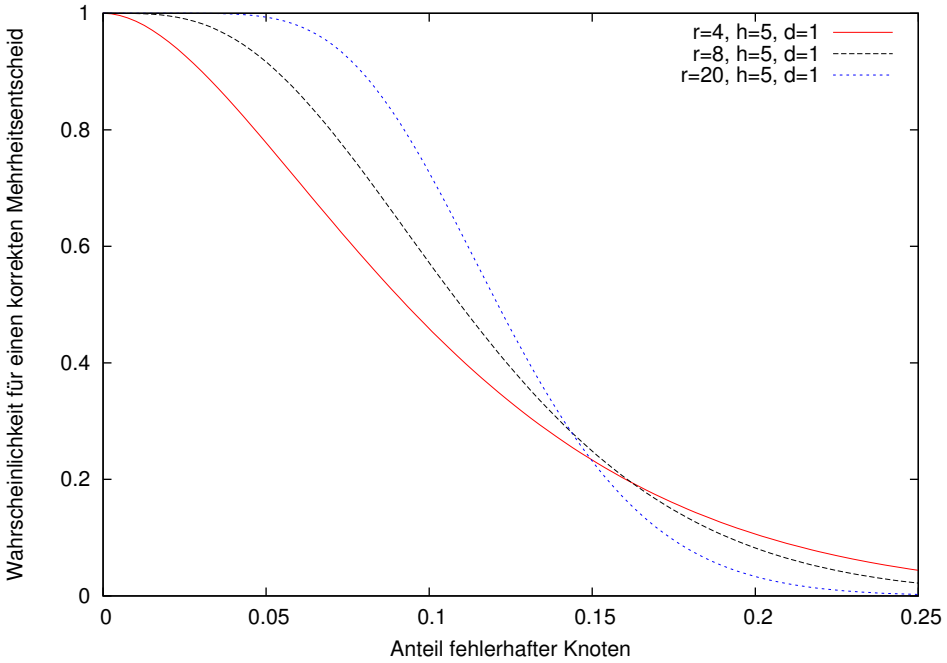


Abbildung 5.6: Wahrscheinlichkeit eines korrekten Mehrheitsentscheids in einer DHT unter Berücksichtigung des Routings bei byzantinischem Fehlermodell (vgl. Formel (5.5))

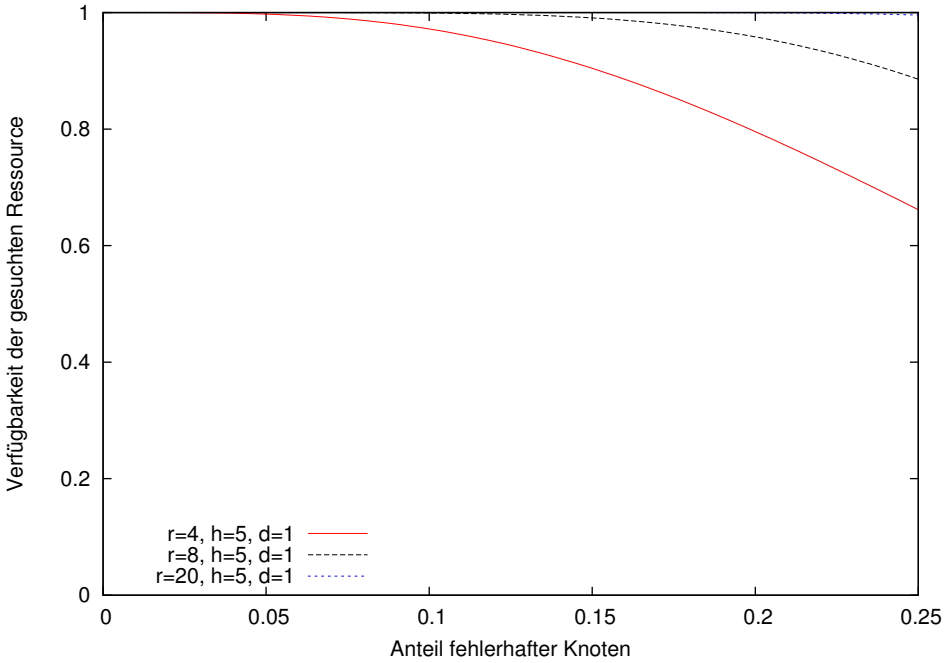


Abbildung 5.7: Verfügbarkeit von Ressourcen in einer DHT unter Berücksichtigung des Routing mit byzantinischem Fehlermodell und einem Fail-Stop-Fehlermodell bei der Datenhaltung (vgl. Formel (5.6))

Datenhaltung hingegen ein Fail-Stop-Fehlermodell angenommen werden kann. Dann ergibt sich die Verfügbarkeitswahrscheinlichkeit für eine DHT aus der Formel (5.4) in Verbindung mit (5.1) zu:

$$1 - (1 - (1 - f)^h)^{d \cdot r} \tag{5.6}$$

Eine Darstellung mit exemplarischen Werten erfolgt in Abb. 5.7, wobei sich zeigt, dass die Verfügbarkeit wesentlich besser als bei einem rein byzantinischen Fehlermodell ist.

5.3 Zusammenschau P2P-spezifischer Angriffe

In diesem Abschnitt wird die Robustheitsbetrachtung um P2P-spezifische Angriffe erweitert, bei welchen die spezifischen Eigenschaften von P2P-Systemen ausgenutzt werden. Bei der Diskussion der Fehlertoleranz im vorigen Abschnitt, bei der Aussagen über die Verfügbarkeit von Ressourcen und die Wahrscheinlichkeit eines korrekten Routing getroffen werden konnten, wurde jeweils eine "statische" Betrachtung vorgenommen unter der Annahme, die Anzahl fehlerhafter Knoten sei bekannt. Bei den P2P-spezifischen Angriffen wird insbesondere die Dynamik und die Umgebungsbedingungen eines P2P-Systems mit einbezogen.

Die Problematik P2P-spezifischer Angriffe wurde bereits zu Beginn des "P2P-Booms" erkannt. Zu den ersten Arbeiten in diesem Bereich zählen insbesondere [Sit & Morris 2002] und [Castro et al. 2002a]. Ausgehend von diesen fokussiert diese Arbeit auf grundlegende Angriffe, die bei P2P-Netzen im Allgemeinen und vor allem bei DHTs möglich sind.

Gegebenenfalls sind in spezifischen Systemen noch weitere Angriffe möglich wie sie exemplarisch in Abschnitt 5.3.4 diskutiert werden. Generelle Angriffe, wie ein Denial-of-Service-Angriff (DoS-Angriff) auf Netzwerkebene mit dem Ziel einzelne Knoten auszuschalten, sind nicht P2P-spezifisch und werden daher auch nicht weiter verfolgt.

Im Folgenden werden zunächst potentielle Angriffsziele und im Anschluss spezifische Angriffsmethoden dargelegt. Dies unterscheidet sich von der Mehrheit anderer Arbeiten, in welchen keine Differenzierung von Zielen und eigentlichen Angriffen stattfindet.

5.3.1 Angriffsziele

Die Angriffsziele in P2P-Systemen sind vielfältig. Daher wird eine Kategorisierung hinsichtlich der Art und dem Wirkungsgrad vorgenommen. Die Angriffsziele können ihrer Art nach wie folgt unterschieden werden:

- **Störung:** Ein Angreifer kann versuchen, ein P2P-System zu stören und somit dessen normale Funktionsweise zu unterbinden bzw. die Leistung des Systems wie Latenzzeiten etc. merklich zu beeinflussen. So könnte es bspw. im Interesse bestimmter Unternehmen sein, die Verbreitung von Inhalten so zu verlangsamen, dass die Attraktivität eines P2P-Systems bei den Nutzern sinkt[8].

- **Überwachung:** Ferner kann es das Ziel eines Angreifers sein, den Zugriff auf Ressourcen oder auch das Routing in einem P2P-System zu überwa-

[8] vgl. hierzu "kommerzielle Störer" wie [WWW MediaDefender]

chen. Dabei bleiben die Routing-Funktionalität und Inhalte des P2P-Systems erhalten. Inhalteanbieter aber auch staatliche Stellen könnten bspw. daran Interesse haben, wer auf welche Inhalte zugreift (vgl. insofern auch Abschnitt 6.4.3).

– **Kontrolle:** Im Gegensatz zur Überwachung kann ein Angreifer auch die Kontrolle über Funktionen, Inhalte oder Ressourcen anstreben. Durch Modifikation einer DHT kann ein Angreifer bspw. versuchen, alle Anfragen für einen Schlüssel auf bösartige Knoten umzuleiten.

Die Angriffsziele sind dabei nicht immer disjunkt, so kann ein Kontrolle gegebenenfalls auch zur Störung genutzt werden.

Weiterhin können die Angriffsziele hinsichtlich ihres Wirkungsgrads unterschieden werden:

– **Lokale Angriffsziele:** Handelt es sich um einen lokalen Angriff, versucht ein Angreifer gezielt die Kommunikation *von* oder *zu* einem bestimmten Knoten zu stören, zu überwachen oder zu kontrollieren. In der Literatur spricht man in diesem Zusammenhang auch von einer so genannten *Eclipse-Attacke*, da ein Knoten in gewissem Sinne ausgeblendet wird [Singh et al. 2004].

– **Globale Angriffsziele:** Bei globalen Angriffen zielt der Angriff auf die Störung, Überwachung oder Kontrolle des Gesamtsystems ab. Es ist dabei im Gegensatz zu lokal ausgeprägten Angriffen nicht das Ziel, spezifische Knoten oder Inhalte auszuschalten, sondern vielmehr das System als Ganzes zu kontrollieren.

Die genannten Angriffsziele betreffen das P2P-System und die Funktionen des selbigen. Darüber hinaus kann ein P2P-System auch als Zwischenstation bzw. zur Verschleierung von Angriffen dienen. So kann bspw. mittels des P2P-Systems ein verteilter Störungsangriff (engl. Distributed DoS) initiiert werden. Indem ein bzw. mehrere bösartige Knoten eines P2P-Systems fälschlicherweise auf einen zu attackierenden Zielknoten verweisen, wird dieser von anderen gutartigen Knoten des P2P-Systems kontaktiert und somit gegebenenfalls überlastet, wobei der attackierte Knoten nicht Teil des P2P-Systems sein muss [Naoumov & Ross 2006].

5.3.2 Angriffsmethoden

Um die genannten Angriffsziele zu verfolgen, können verschiedene Angriffsmethoden genutzt werden. Im Folgenden werden diese vorgestellt und deren Eignung für die obigen Ziele diskutiert. Die Methoden werden dabei in primäre und

sekundäre unterschieden. Bei den folgenden Angriffsmethoden wird vorausgesetzt, dass ein Angreifer einen oder teilweise auch mehrere Knoten innerhalb des P2P-Netzes kontrolliert.

Zu den primären Angriffsmethoden zählen:

- **Fehlleiten von Nachrichten:** Indem ein Angreifer Nachrichten nicht oder an einen falschen Empfänger weiterleitet, kann er die korrekte Funktion eines P2P-Netzes beeinflussen.

- **Ressourcen/Knoten-Kontrolle:** Um eine bestimmte Ressource zu kontrollieren, kann ein Knoten versuchen sich an der entsprechenden Stelle des Netzes zu platzieren. Vor allem bei strukturierten Netzen, die P2P-spezifische Kennungen nutzen und eine dementsprechende Strukturierung aufweisen, ist dies erfolgversprechend, indem ein Angreifer passende Knotenkennungen wählt[9].

- **Churn-Angriff:** Die selbstorganisierenden Mechanismen in P2P-Systemen ermöglichen neue Knoten automatisiert zu integrieren und ausgefallene Knoten entsprechend wieder aus den Routing-Tabellen zu entfernen. Treten in ein Netz in kurzer Zeit viele Knoten ein und wieder aus, kann dies für einen Angriff genutzt werden, da durch die Verwaltung der Ein- und Austritte eine erhöhte Netzlast entsteht. Unstrukturierte Netze sind davon kaum betroffen. Bei strukturierten Netzen müssen jedoch die Routing-Tabellen anderer Knoten angepasst werden, so dass die Struktur des Netzes erhalten bleibt. In [Rhea et al. 2004] werden verschiedene DHTs hinsichtlich dieses Angriffs untersucht. Diese Angriffsmethode wird teilweise auch als "Rapid Join/Leave Attack" bezeichnet [Sit & Morris 2002; Awerbuch & Scheideler 2006].

Mittels dieser elementaren Angriffsmethoden ist es möglich, die Angriffsziele Störung, Überwachung und Kontrolle umzusetzen. Je nach Ausprägung handelt es sich dann um einen lokalen oder globalen Angriff.

Nutzt ein Angreifer lediglich einen oder wenige Knoten in Verbindung mit den genannten primären Angriffsmethoden, geht dadurch nur eine begrenzte Gefahr aus, die im Wesentlichen auf Basis der Fehlertoleranz-Betrachtung im vorigen Abschnitt abgeschätzt werden kann. Durch die Kombination mit den folgenden sekundären Angriffsmethoden kann jedoch eine katalysierende Wirkung entstehen, durch welche die Gefahr erheblich zunimmt:

[9] In der englischen Literatur wird hierfür der Ausdruck "Root-Spoofing" verwendet, da der Angreifer versucht die Wurzel eines Schlüssels zu kontrollieren.

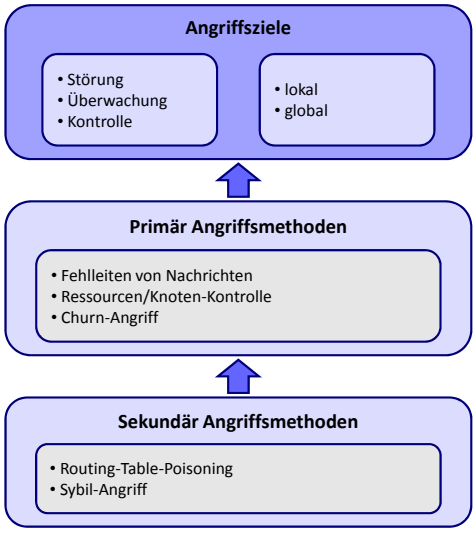


Abbildung 5.8: Zusammenhang zwischen Angriffszielen sowie primären und sekundären Angriffsmethoden

- **Routing-Table-Poisoning:** Durch die Verbreitung falscher Routing-Tabelleneinträge kann ein Angreifer die Weiterleitung von Nachrichten zu seinen Gunsten verändern [Sit & Morris 2002]. Können gutartige Knoten dies nicht detektieren, leiten diese Nachrichten unabsichtlich zu den falschen (in der Regel bösartigen) Knoten weiter.

- **Sybil-Angriff:** Gelingt es einem Angreifer unter verschiedenen Identitäten zu agieren, d.h. mehrere Knoten zu betreiben, wird dies als Sybil-Angriff bezeichnet [Douceur 2002]. Mittels einer solchen Attacke kann es dem Angreifer insbesondere gelingen Redundanzmechanismen auszuhebeln, da sich dadurch das Verhältnis von bösartigen und gutartigen Knoten verändert. Eine vertiefte Diskussion dieses Angriffs erfolgt in Abschnitt 5.4.

Die dargelegte Klassifikation von Angriffszielen und Angriffsmethoden unterscheidet sich von anderen Arbeiten insofern, dass sie eine differenzierte und umfassende Betrachtung des Themenkomplexes erlaubt und keine Annahmen über den Angreifer a priori getroffen werden müssen. Andere Klassifikationen wie zum Beispiel in [Singh et al. 2004], die besagen, dass eine Eclipse-Attacke allgemeiner als der Sybil-Angriff sei, sind hingegen nur unter bestimmten Annahmen zutreffend. In Abb. 5.8 sind die Angriffsziele und -methoden nochmals graphisch zusammengefasst dargestellt.

5.3.3 Bewertung und grundlegende Abwehrprinzipien

In diesem Abschnitt erfolgt eine Bewertung der Angriffsmethoden und eine Darlegung grundlegender Abwehrmechanismen. Soweit keine explizite Unterscheidung erfolgt, beziehen sich die folgenden Ausführungen sowohl auf unstrukturierte als auch strukturierte P2P-Netze. Dabei bleibt jedoch zu beachten, dass die Indices, wie in Abschnitt 3.3.2 ausgeführt, bei unstrukturierten Netzen lokal verwaltet werden. Insofern beschränkt sich die Gefährdung dort in der Regel auf Routing-Angriffe.

Primäre Angriffsmethoden – Ressourcen/Knoten-Kontrolle: Um bestimmte Teile eines P2P-Netzes zu kontrollieren, ist es notwendig, für die (entsprechenden Teile des) Indices zuständig zu sein. Bei unstrukturierten Netzen ist dies aufgrund der lokalen Indices nicht möglich. In strukturierten Netzen bestimmt sich die Zuständigkeit anhand P2P-spezifischer Kennungen. Um gezielt Schlüssel zu kontrollieren, muss es einem Angreifer gelingen, für diese zuständig zu sein.

Insofern sollte sich ein Angreifer diese Kennungen nicht selbstständig aussuchen können. Vielmehr sollten die Kennungen zufällig vergeben werden und die Anzahl der Kennungen, die ein Angreifer pro Zeiteinheit erzeugen kann, begrenzt sein. Ferner sollte es anderen Knoten möglich sein, die korrekte Vergabe zu verifizieren (vgl. [Sit & Morris 2002]).

Werden diese Maßnahmen durchgesetzt, ist einem Angreifer nicht möglich, gezielt bestimmte Bereiche eines Kennungsraums zu beherrschen. Zudem kann hierdurch auch das Fehlleiten von Nachrichten erschwert werden, wie im Folgenden noch erläutert wird.

Eine Möglichkeit, eine zufällige Knotenkennung zu bestimmen, besteht darin, die Kennung aus der IP-Adresse und dem Port des Knotens zu berechnen. Durch Einsatz einer konsistenten Hash-Funktion kann eine entsprechende gleichmäßige Verteilung über den Schlüsselraum erreicht werden. Durch Anwenden der Hash-Funktion kann ein anderer Knoten diese Berechnung auch nachvollziehen. Es ist einem Knoten jedoch möglich, durch Wechseln des Ports oder der IP-Adresse unterschiedliche Knotenkennungen zu generieren. Da die Vergabe von Knotenkennungen auch im Rahmen des Sybil-Angriffs ein zentrale Rolle einnimmt, erfolgt die weitere Diskussion in Abschnitt 5.4.

Primäre Angriffsmethoden – Fehlleiten von Nachrichten: In einem offenen P2P-System kann das Fehlleiten oder Unterdrücken von Nachrichten nicht vollständig verhindert werden. Andererseits kann die entstehende Gefahr entsprechend der Fehlertoleranz-Betrachtungen im vorigen Abschnitt abgeschätzt werden, sofern der Anteil bösartiger Knoten bekannt ist. Wie bereits oben ausgeführt,

kann die Robustheit gegenüber Fail-Stop-Fehlern, d.h. auch das Unterdrücken von Nachrichten, durch ein iteratives Routing erhöht werden.

Da unstrukturierte Netze keine spezifischen Kennungen aufweisen, können Abwehrstrategien dort nur auf Basis der Netzwerkadressen der Knoten stattfinden. So kann bspw. versucht werden beim Routing möglichst unterschiedliche Netze bzw. Autonome Systeme einzubeziehen. Vor allem bei Anonymisierungsdiensten wird dieses Verfahren angewandt (vgl. [Freedman & Morris 2002]). Dabei bleibt jedoch zu beachten, dass sich dies negativ auf die Leistung auswirken kann, da möglichst "nahe" Knoten nicht mehr bevorzugt werden.

Bei strukturierten Netzen ist das Weiterleiten der Nachrichten abhängig von den Knotenkennungen. Insofern sollte die Vergabe der Knotenkennungen durch eine verifizierbare Methode wie oben ausgeführt stattfinden, da ansonsten die Knotenkennungen keine Maßgabe zur Absicherung bietet. Strukturierte Netze weisen in der Regel Invarianten auf, die beim korrekten Weiterleiten der Nachrichten erfüllt sein müssen. So reduziert sich der Abstand zwischen dem gesuchten Schlüssel und den Knoten auf dem Pfad kontinuierlich.

Auch wenn die Vergabe der Kennungen verifizierbar erfolgt, unterscheiden sich die Möglichkeiten, die ein Knoten hat, sich in einen Pfad zum Zielknoten zu positionieren je nach Protokoll. Wie in [Castro et al. 2002a] näher ausgeführt, ist die Wahrscheinlichkeit bei strikten Protokollen wie Chord geringer, dass sich ein bösartiger Knoten in einem Pfad positionieren kann als bei P2P-Netzen wie Pastry oder Kademlia, da bei strikten Protokollen die Struktur fest vorgegeben ist, so dass nur ein möglicher Pfad existiert. Die letztgenannten Protokolle lassen hingegen in gewissen Grenzen eine flexible Auswahl der Knoten zu, um die Leistung des P2P-Netzes hinsichtlich Latenz etc. zu optimieren. So werden bei Kademlia vornehmlich Knoten gewählt, die nah im Sinne der Latenz sind und bereits lange am Netz teilnehmen (vgl. auch Abschnitt 2.4.3).

Um die Gefahr einzuschränken und dennoch die Vorteile der flexiblen Knotenauswahl nutzen zu können, wird in [Castro et al. 2002a] die Verwendung von zwei Routing-Tabellen vorgeschlagen – eine flexible Routing-Tabelle und eine zweite so genannte Constrained Routing-Tabelle, in welcher eine strikte Reihenfolge vorgeben ist. Im Regelfall erfolgt die Weiterleitung mittels der flexiblen Routing-Tabelle. Dabei wird jeweils ein Test durchgeführt, ob die Konzentration an Knotenkennungen als normal zu betrachten ist oder auf einen Angriff hin deutet. Der Test beruht dabei auf der Tatsache, dass der Kennungsraum in der Regel gleichmäßig besetzt ist und somit der Abstand zwischen den benachbarten Knoten in etwa gleich sein sollte. Deutet der Test auf eine ungewöhnliche Konstellation an Knotenkennungen hin, findet das Routing mittels der Constrained Routing-Tabelle statt. Die Autoren zeigen, dass durch diese Technik in Verbin-

dung mit disjunkten Routing-Pfaden mit einer Wahrscheinlichkeit von mehr als 99,9 % bei bis zu 25 % bösartiger Knoten und 32 disjunkten Pfaden das Routing erfolgreich ist.

In [Hildrum & Kubiatowicz 2007] wird ein weiteres Verfahren vorgeschlagen, welches nach wie vor flexible Routing-Tabellen ermöglicht und dennoch robust gegenüber Angriffen ist. Es handelt sich dabei um ein iteratives Routing-Verfahren, bei welchem in jedem Schritt mehrere potentielle Knoten kontaktiert werden und die jeweils nächsten im Sinne der Latenzzeit für das weitere Routing genutzt werden. Dem Verfahren liegt die Annahme zugrunde, dass die bösartigen Knoten gleichmäßig im Netz verteilt sind.

Das Ziel eines Churn-Angriffs besteht darin, die Funktion des P2P-Netzes maßgeblich zu stören. In [Rhea et al. 2004] findet eine ausführliche Darstellung der Auswirkung eines Churn-Angriffs auf verschiedene DHTs statt. Ferner werden verschiedene Eigenschaften der DHTs identifiziert, die sich auf die Effektivität eines solchen Angriffs auswirken. Unstrukturierte Netze können durch einen Churn-Angriff kaum gestört werden, da diese keine spezifische Struktur aufweisen und insofern auch keine Wartung der Routing-Tabellen nötig ist.

Sekundäre Angriffsmethoden: Die Bedeutung von den sekundären Angriffsmethoden liegt vor allem darin, die notwendige Grundlage für die primären Angriffsmethoden zu schaffen bzw. deren Effektivität zu erhöhen, um letztlich die spezifizierten Angriffsziele zu verfolgen. Insofern handelt es sich um eine Kaskadierung von Angriffsmethoden.

Durch die Verbreitung fehlerhafter Routing-Tabelleneinträge, d.h. *Routing-Table-Poisoning*, kann ein Angreifer versuchen, den Einfluss in den Routing-Tabellen gutartiger Knoten zu erhöhen, so dass mehr Nachrichten über ihn geleitet werden. Erschwerend kommt hinzu, dass teilweise auch gutartige Knoten die fehlerhaften Routing-Tabelleneinträge weiterleiten. Letztlich kann ein Angreifer mittels einer solchen Attacke sukzessiv mehr Nachrichten fehlleiten und gegebenenfalls auch bestimmte Schlüssel kontrollieren, da die eigentlich zuständigen Knoten nicht mehr erreichbar sind. Auch in unstrukturierten Netzen ist ein Routing-Table-Poisoning möglich, da auch diese Protokolle, insbesondere beim Beitritt eines Knotens Routing-Tabelleneinträge austauschen. Wie auch beim Fehlleiten von Nachrichten kann bei strukturierten Netzen ein solcher Angriff durch verifizierbare Vergabe von Knotenkennungen und strikte Routing-Tabellen verhindert werden.

Ist es einem Angreifer möglich, unter beliebig vielen Identitäten, d.h. mit beliebig vielen Knoten, an einem P2P-Netz teilzunehmen, spricht man von einem *Sybil-Angriff*. Der Angreifer kann dadurch einen wesentlichen Einfluss ausüben.

Gelingt es nicht, die Anzahl zu begrenzen oder diese zusätzlichen Identitäten zu detektieren, kann ein Angreifer alle Schutzmechanismen aushebeln, da jegliche Redundanzmechanismen nur dann effektiv sind, wenn eine maximaler Anteil bösartiger Knoten bekannt ist. Insofern geht von einem Sybil-Angriff die größte Bedrohung aus.

Ferner kann der Sybil-Angriff mit dem Routing-Table-Poisoning kombiniert werden (Genau genommen ist ein Routing-Table-Poisoning-Angriff ohne zusätzlichen Sybil-Angriff nicht möglich.), wodurch der immense Einfluss nochmals wesentlich verstärkt wird, wie in Abschnitt 5.5.2 gezeigt wird.

Zwischenergebnis

Insgesamt ergeben sich folgende Grundsätze, um einen Angriff zu erschweren:

- Daten sollten redundant gespeichert werden.
- Alternative Routing-Pfade sind essentiell.
- Das Routing sollte iterativ erfolgen und die entsprechenden Invarianten sollten geprüft werden.
- Die Vergabe der Knotenkennungen sollte reglementiert und verifizierbar sein.

Die Zusammenschau der möglichen Angriffsmethoden ergibt, dass insbesondere der Sybil-Angriff eine große Gefahr für P2P-Netze darstellt, da bei einem solchen keine Abschätzung hinsichtlich des Anteils bösartiger Knoten mehr möglich ist und somit die Bewertungen, wie sie auch im Rahmen der Fehlertoleranz stattfanden, ins Leere laufen.

5.3.4 Weitere Angriffsmethoden und -ziele

Betrachtet man spezifische P2P-Systeme, sind noch weitere Angriffe möglich. Insofern muss eine Analyse spezifisch für jedes P2P-System durchgeführt werden. An dieser Stelle soll jedoch lediglich auf weitere Arbeiten hingewiesen werden. Eine vertiefte Diskussion dieser Problematiken kann im Rahmen dieser Arbeit nicht erfolgen. Vielmehr bilden die in dieser Arbeit dargelegten Analysen und Verfahren eine Basis für die Bewertung dieser spezifischen Angriffe. So erfordert bspw. auch ein Anreizsystem ein "robustes" P2P-System bzw. in den Arbeiten werden in der Regel Annahmen zum maximalen Anteil bösartiger Knoten getroffen.

In [Dhungel et al. 2008] wird dies bspw. zu BitTorrent diskutiert. Bei BitTorrent kann das Herunterladen einer Datei gestört werden, indem von bösartigen Knoten falsche Dateiblöcke geliefert werden oder der Besitz von Dateiblöcken

vorgetäuscht wird, ohne diese letztlich zur Verfügung zu stellen. Anderen Knoten können solch ein Verhalten durch Prüfsummen bzw. Ausbleiben von Daten zwar erkennen, dennoch wird das Herunterladen verlangsamt und es führt somit zu einer Störung.

Die Überlastung von DHT-Knoten mit zu vielen oder zu großen Einträge wird nebst entsprechender Lösungsstrategien unter anderem in [Rhea et al. 2005b] diskutiert.

Da Identitäten in P2P-Systemen in der Regel kostenfrei sind, können bösartige Knoten an einem P2P-System teilnehmen, ohne selbst Ressourcen beizutragen (engl. Free-Riding). Ebenso ist es bösartigen Knoten bei Reputationssystemen unter Umständen möglich, sich negativer Bewertungen durch Generierung einer neuen Identität zu entledigen (engl. Whitewashing). Dies betrifft auch Anreizsysteme wie "Tit-for-Tat". Hierzu sei auf die Arbeiten [Buragohain et al. 2003] und [Feldman et al. 2004] hinsichtlich Anreizsystemen verwiesen. Die Arbeit [Feldman et al. 2006] thematisiert die Free-Riding- und Whitewashing-Problematik.

5.4 Der Sybil-Angriff

Wie im vorigen Abschnitt dargelegt, hat ein Sybil-Angriff das Potential sämtliche Redundanzmechanismen zu unterminieren. Ziel dieses und der beiden folgenden Abschnitte ist es, die Gefahren, die von einem solchen Angriff ausgehen, durch simulative Analysen und Messungen in realen Netzen in Kontext zu den notwendigen Ressourcen zu setzen. Hierzu werden in diesem Abschnitt Grundlagen und verwandte Arbeiten diskutiert. In den folgenden beiden Abschnitten werden Analysen und Abwehrstrategien insbesondere ein neuartiges Selbstregistrierungsverfahren präsentiert.

5.4.1 Grundlagen und Definition

Der Begriff Sybil-Angriff[10] wurde durch die grundlegende Arbeit von J. Douceur geprägt [Douceur 2002].

> *"If a single faulty entity can present multiple identities, it can control a substantial fraction of the system, thereby undermining this redundancy."* aus [Douceur 2002]

Gelingt es einer *einzelnen Entität*, in einem System unter *mehreren Identitäten* zu agieren, handelt es sich nach Douceur um einen *Sybil-Angriff*. Dabei ist insbesondere problematisch, dass Redundanzmechanismen, wie sie bspw. in Abschnitt 5.2

[10] Der Begriff Sybil geht auf die Romanfigur Sybil Dorsett zurück, die unter einer multiplen Persönlichkeitsstörung litt [Schreiber 1995].

diskutiert wurden, ins Leere laufen können, da die Operationen nicht auf verschiedenen Entitäten ausgeführt werden, sondern auf einer und somit die Annahmen über die Unabhängigkeit der Ausfälle sowie den Anteil fehlerhafter Knoten inkorrekt sind. Die zusätzlichen Identitäten einer Entität werden auch als *Sybils* bezeichnet (vgl. u.a. [Cheng & Friedman 2005]).

Grundlegende Erkenntnisse von Douceur: In seiner grundlegenden Arbeit spezifiziert Douceur ein simples formales Modell, das aus einer Menge Entitäten besteht, die direkt miteinander verbunden sind und das Broadcast-Kommunikation vorsieht. Der Nachrichtenversand wurde dabei als zuverlässig definiert und ist unabhängig von den Ressourcen einer Entität. Die zur Verfügung stehenden Rechenressourcen der Entität des Angreifers werden im Verhältnis zu den Ressourcen der schwächsten Entität angegeben. Mittels dieses Modells kann Douceur schließlich folgende Ergebnisse zeigen:

- Wenn eine Überprüfung der Ressourcen einer Entitäten nicht simultan erfolgt, kann eine bösartige Entität eine beliebige Menge an gefälschten Identitäten präsentieren, da die nötigen Ressourcen mehrfach verwendet werden können.
- Bei der indirekten Verifizierung, d.h. wenn eine Identität durch eine bereits akzeptierte Identität bestätigt wird, genügt eine ausreichend große Menge an bösartigen Entitäten, um eine beliebige Anzahl von Identitäten zu fälschen.
- Sind die zur Verfügung stehenden Ressourcen der Entitäten unterschiedlich, kann eine bösartige Entität eine konstante Anzahl Identitäten fälschen, nämlich so viele, wie sich durch das Verhältnis zwischen minimal nötigen Ressourcen einer Entität und den Ressourcen der bösartigen Entität ergibt.

Daraus schließt Douceur, dass für eine ressourcenbasierte Verifizierung der Identitäten die Ressourcen der Entitäten nahezu gleichverteilt sein müssen und diese auch simultan überprüft werden müssen. Letztlich argumentiert Douceur, dass diese Bedingungen in massiv verteilten Systemen, wie es P2P-Systeme sind, nicht realisierbar sind. Nach seiner Auffassung kann somit nur die zentralisierte Vergabe von Identitäten durch eine dritte vertrauenswürdige Partei in Verbindung mit Zertifikaten als Sybil-resistent angesehen werden.

Anwendungsbereich: Den Arbeiten von Douceur lagen P2P-Systeme zugrunde. Aufgrund des abstrakten Modells können die Ergebnisse jedoch auch in anderen Bereichen Anwendung finden.

So zeigen Newsome et al. wie sich ein Sybil-Angriff in Sensornetzen auswirkt [Newsome et al. 2004]. Auch bei mobilen Ad-hoc-Netzen kann es zu einem Sybil-Angriff kommen [Piro et al. 2006]. Aufgrund der geographischen und physikalischen Beschränkungen solcher Netze sind die Auswirkungen dort meist geringer bzw. es können Abwehrmechanismen auf Basis dieser Beschränkungen realisiert werden. Im Gegensatz dazu operieren P2P-Systeme meist auf Grundlage des Internet und somit auf globalem Maßstab.

Bei der Gestaltung von Reputationssystemen können Sybils auch eine entscheidende Rolle spielen. Cheng und Friedman zeigen in ihrer grundlegenden Arbeit [Cheng & Friedman 2005], dass es keine symmetrischen Reputationsfunktionen gibt, die resistent gegenüber einem Sybil-Angriff sind. Der Beweis beruht auf der Tatsache, dass ein Angreifer zu jedem existierenden Graphen, der durch eine symmetrische Reputationsfunktion entsteht, eine Kopie erstellen kann. Hat ein Angreifer nicht den höchsten Reputationswert, so kann er eine exakte Kopie des existierenden Graphen erstellen. Diese Kopie enthält sodann auch mindestens einen Knoten, dessen Reputationswert maximal ist. Da die Reputationsfunktion als symmetrisch angenommen wurde, kann nicht zwischen dem ursprünglichen und dem kopierten Graphen unterschieden werden und der Angreifer ist somit im Besitzt eines Knotens mit dem höchsten Reputationswert. Eine Differenzierung ist erst durch eine asymmetrische Reputationsfunktion möglich, bei der so genannte (vertrauenswürdige) Fixknoten zum Einsatz kommen.

5.4.2 Bestehende Lösungsansätze

Neben der Arbeit von Douceur wurden die Herausforderungen, die durch Sybils entstehen, in weiteren Arbeiten aufgegriffen. Die bestehenden Lösungsansätze können in die vier Kategorien Zertifizierung durch vertrauenswürdige Dritte, soziale Netze, Ressourcenprüfung und Ableitung von Identitäten unterteilt werden. Darüber hinaus existieren noch eine Reihe von Arbeiten, in welchen die Problematik durch Sybil-Angriffe zwar Erwähnung findet, jedoch keine Lösung präsentiert wird (vgl. [Levine et al. 2006]). Eine Darstellung bestehender Lösungsansätze findet sich auch in der überblicksartigen Arbeit [Levine et al. 2006].

Zertifizierung durch vertrauenswürdige dritte Instanz: Entsprechend der Ergebnisse von Douceur wurde von zahlreichen Arbeiten, wie [Rowstron & Druschel 2001], [Castro et al. 2002a], [Zhao et al. 2004] oder [Hildrum & Kubiatowicz 2007] eine vertrauenswürdige dritte Instanz (engl. Trusted Third Party) vorgesehen, die für die Ausgabe von Identitäten im P2P-System zuständig ist.

Diese Instanz muss die Eindeutigkeit der Identitäten sicherstellen und dafür Sorge tragen, dass *eine* Entität nur in den Besitz *einer* Identität gelangt. Ferner

muss den Knoten eine Möglichkeit gegeben werden, die Korrektheit einer Identität zu überprüfen. Bei der dritten Instanz kann es sich um eine Einzelne oder um eine Hierarchie von vertrauenswürdigen Instanzen handeln. Das Konzept ist daher vergleichbar einer Public Key Infrastructure (PKI). Wie bei einer PKI auch, kann die Identität durch Signaturen und entsprechende öffentliche und private Schlüssel gesichert werden. Den Knoten muss hierzu der öffentliche Schlüssel der vertrauenswürdigen Instanz bekannt sein.

Nachteilig bei dieser Lösung ist, dass der völlig dezentrale Charakter von P2P-Systemen nicht mehr gegeben ist und ein Single-Point-of-Failure entsteht. Die Generierung der Identitätsinformationen erfolgt zwar einmalig, so dass der Betrieb des P2P-Systems unabhängig von der Erreichbarkeit der vertrauenswürdigen dritten Instanz ist. Lediglich neue Knoten können beim Ausfall der Instanz nicht dem P2P-System beitreten. Wollen allerdings zu einem Zeitpunkt viele Knoten dem P2P-System beitreten, kann eine zentralisierte Instanz problembehaftet sein. So führte die Aktualisierung eines weit verbreiteten Betriebssystems im August 2007 dazu, dass innerhalb kurzer Zeit eine große Anzahl von Knoten aus dem System Skype austraten, um kurz darauf sich wieder mit diesem zu verbinden, so dass es in der Folge zu einer Überlastung der zentralen Login-Server kam [Arak 2007].

Unklar bleibt in den Arbeiten, anhand welcher Kriterien diese zentralisierte Instanz die Verschiedenheit von Entitäten erkennt. Ferner bleibt meist offen, wer eine solche vertrauenswürdige Instanz betreibt. In [Castro et al. 2002a] wird vorgeschlagen, für die Ausstellung von Identitäten einen monetären Betrag zu verlangen, der gleichzeitig wieder zum Betrieb der vertrauenswürdigen Instanz dient. Folgt man dieser Argumentation, kann es einer bösartigen Entität durchaus gelingen, in den Besitz mehrerer Identitäten zu gelangen. Allerdings wird die Anzahl durch das zur Verfügung stehende Kapital begrenzt. In diesem Sinne kann jedoch auch die Ressourcenbeschränkung in Abschnitt 5.6 aufgefasst werden, ohne dass dort eine zentrale Instanz von Nöten ist.

Soziale Netzwerke: Bei dem vorgenannten Lösungsansatz kommt eine dedizierte vertrauenswürdige dritte Instanz zum Einsatz, bei der insbesondere die Betreiberfrage ungeklärt bleibt und die darüber hinaus einen Single-Point-of-Failure darstellt. Um diese Probleme zu umgehen, wurde daher von mehreren Arbeiten die Nutzung von so genannten sozialen Netzwerken vorgeschlagen. Dabei wird neben dem eigentlichen P2P-Netz ein zweiter Graph gepflegt, in welchem die Vertrauensbeziehungen der Nutzer untereinander einfließen. Ein Vertrauen zwischen zwei Nutzern wird dabei durch eine Kante in dem sozialen Graphen repräsentiert.

In [Danezis et al. 2005] wird hierzu ein so genannter Bootstrap Graph aufgebaut. Für den Beitritt wird jeweils ein Knoten genutzt, zu dem bereits über einen externen Kanal eine Vertrauensbeziehung etabliert wurde. Durch ein modifiziertes Chord-Routing fließen die Vertrauensbeziehungen ein, so dass nur begrenzt viele Sybils dem "gutartigen Teil des Netzes" beitreten können.

Dem zweiten Ansatz in [Yu et al. 2006] liegt ein soziales Netz zugrunde, das über externe Kommunikationskanäle und entsprechende kryptographische Verfahren etabliert wird. Ausgehend von der Annahme, dass Sybils nur über wenige Kanten mit gutartigen Knoten im sozialen Netz verbunden sind, entwerfen die Autoren ein Verfahren, mittels dessen die Anzahl der Sybils begrenzt werden kann, indem die Knoten entsprechend der Kanten des sozialen Graphen gruppiert werden. Eine optimierte Variante des Verfahrens wird in [Yu et al. 2008] sowie eine Abwandlung in [Lesniewski-Laas 2008] präsentiert.

Nachteilig bei den Verfahren wirkt sich die Tatsache aus, dass ein soziales Netz nötig ist, welches über einen externen Kommunikationskanal etabliert werden muss. Ferner ist für die Etablierung der Vertrauensverhältnisse in beiden Fällen ein Schlüsselaustausch notwendig. In [Yu et al. 2006] argumentieren die Autoren zwar, dass ein Schlüssel problemlos bspw. per Telefon übermittelt werden könnte. Dennoch ist der Aufwand für Nutzer und das resultierende Akzeptanzproblem nicht zu vernachlässigen.

Bei diesen Ansätzen wird die Annahme getroffen, dass jede gutartige Entität zu *einem* Nutzer gehört und bösartige Entitäten zwar beliebig viele Knoten im sozialen Netz besitzen können, jedoch nur wenige Verbindungen, d.h. Vertrauensbeziehungen zu gutartigen Knoten haben. Fraglich bleibt jedoch, ob diese Annahmen zutreffen.

Implizit wird auch unterstellt, dass bereits Personen, die am fraglichen P2P-System teilnehmen, über einen externen Kommunikationskanal bekannt sind. Bei Telefoniediensten wird dies in der Regel noch gegeben sein, doch bei Dateitausch-Systemen oder Anonymisierungsdiensten ist dies nicht ohne Weiteres der Fall.

Ressourcenprüfung: Besitzt ein bösartiger Knoten mehr als die minimal für eine Entität nötige Menge an Ressourcen, kann er mehrere Identitäten präsentieren. Dennoch kann durch einen Nachweis von Ressourcen – im Folgenden als Ressourcenprüfung bezeichnet – sichergestellt werden, dass die Anzahl generierbarer Identitäten pro Menge zur Verfügung stehender Ressourcen begrenzt ist [Rowaihy et al. 2007, S. 2598]. In mehreren Arbeiten wurde dieser Ansatz aufgegriffen, wobei bereits Douceur die drei Kategorien Speicherplatz, Netzbandbreite und Rechenkapazität vorsah. Des Weiteren werden noch weitere Eigenschaften des Netzwerks wie die Latenz zwischen Knoten genutzt, um eine Unterscheidung

von Entitäten zu ermöglichen.

Unter der Annahme, dass die Rechenkapazität eines Angreifers beschränkt ist, werden in mehreren Arbeiten zur Ressourcenprüfung so genannte kryptographischen Rätsel (engl. Cryptographic Puzzle [Merkle 1978]) genutzt. In [Rowaihy et al. 2007, 2005] entwickeln die Autoren ein Verfahren, bei dem beitretende Knoten mehrere kryptographischen Rätsel lösen müssen, um dem P2P-Netz beitreten zu dürfen. Die Rätsel werden dabei von bereits beigetretenen Knoten gestellt, die in einer Hierarchie organisiert sind. Insofern existiert auch ein designierter Knoten, der die Spitze der Hierarchie bildet. Der Unterschied zu den vorgenannten Verfahren mittels zentralerer vertrauenswürdiger Instanz besteht darin, dass dieses Verfahren keine weiteren, externen Identifikationsmerkmale benötigt. Nachteilig auch bei diesem Verfahren ist der erforderliche zentrale Anker. Ferner bleiben verschiedene Annahmen, die der simulativen Untersuchung zugrunde liegen, wie zum Beispiel die Ressourcen eines Angreifers unklar.

Auch in [Borisov 2006] finden kryptographischen Rätsel Verwendung. Die Knoten müssen dabei regelmäßig, während der üblichen Wartung der Routing-Tabellen des P2P-Netzes, Rätsel lösen. Der präsentierte Ansatz kommt dabei ohne die Verwendung einer zentralen Instanz aus. Jedoch wurden auch bei dieser Arbeit keine Annahmen über die Verteilung der Rechenkapazitäten gemacht, so dass unklar bleibt, welchen Einfluss ein Angreifer nehmen kann.

Das in [Bazzi & Konjevod 2005] vorgeschlagene Verfahren, um Entitäten zu differenzieren, basiert darauf, den Abstand in Form der Latenzzeit zwischen Knoten zu bestimmen. Eine grundlegende Idee dabei ist, dass bösartige Knoten zwar Nachrichten verzögern, aber nicht "beschleunigen" können. Durch so genannte Beacons kann die Latenz zwischen zwei Knoten bestimmt werden, ohne seine eigene Identität preis zu geben. Dem Verfahren liegt die Annahme zugrunde, dass der Anteil bösartiger Beacons begrenzt ist. Fraglich bleibt dabei, durch wen solche Beacons betrieben werden.

Ableitung von Identitäten: Eine besondere Stellung nehmen Netzwerkadressen, genauer IP-Adressen, ein, da es sich dabei nicht um eine Ressource im eigentlichen Sinne handelt. Es ist vielmehr eine Identität auf IP-Ebene, die durch die IANA bzw. untergeordnete Registrierungsstellen zugeteilt wird (vgl. auch Anhang B). Steht einem Angreifer nur eine IP-Adresse zur Verfügung, kann eine eindeutige Knotenkennung durch eine Hash-Funktion berechnet werden, indem die IP-Adresse gehasht wird [Stoica et al. 2001]. Andere Knoten können diese Berechnung sehr leicht nachvollziehen und somit die Knotenkennung verifizieren. Insofern handelt es sich um eine Ableitung von Identitäten, die aus Sicht des P2P-Systems komplett dezentral realisierbar ist. Offen bleiben jedoch die Fra-

gen, wie mehrere Knoten mit der gleichen IP-Adresse betrieben werden können oder was geschieht, wenn ein Angreifer über mehrere IP-Adressen wie bspw. bei IPv6 verfügt (vgl. u.a. [Yu et al. 2006]). Diese Nachteile werden in Abschnitt 5.6.2 vertieft diskutiert bzw. durch das neu entwickelte Selbstregistrierungsverfahren entkräftet.

Anonymisierungsdienste wie Tarzan oder Tor versuchen den Einfluss von Sybils zu reduzieren indem sie Nachrichten durch mehrere Netze respektive Subnetze leiten [Freedman & Morris 2002]. Ein Netz wird bei IPv4 durch einen 16 oder 24 bit IP-Adresspräfix bestimmt. Die Anzahl Sybils wird durch das Verfahren jedoch nicht begrenzt.

5.4.3 Resümee

Bei den vorgenannten Lösungsansätzen, die einen zentralen Anker voraussetzen, bleiben insbesondere betriebliche Fragen offen. So stellt sich die Frage, wer eine zentrale Instanz vertrauenswürdig betreiben kann, wie deren Betrieb finanziert wird und wie diese Entitäten differenzieren kann. Außerdem stellen zentrale Komponenten einen Single-Point-of-Failure dar, der gerade durch P2P-Systeme vermieden werden sollte. Auch die Arbeiten auf Basis sozialer Netze weisen verschiedene Nachteile wie die Etablierung von Vertrauensbeziehungen durch externe Kanäle auf.

Sowohl bei der Arbeit von Douceur als auch anderen Arbeiten erfolgt die Modellierung der begrenzenden Ressourcen wie Rechenleistung und Netzbandbreite nur auf einem abstrakten und daher unzureichendem Niveau, um eine Bewertung der tatsächlichen Gefahren durchführen zu können. Aufgrund der einfachen Modelle bleibt das Verhältnis zwischen begrenzenden Ressourcen und der Anzahl möglicher Sybils unklar und es bleibt fraglich, ob eine geringe Menge Sybils nicht unerheblich bleibt.

Um die tatsächliche Gefahr, die von Sybil-Angriffen ausgeht, korrekt einschätzen zu können, ist eine solche Betrachtung unerlässlich. Dabei bleibt auch zu berücksichtigen, dass selbst vermeintlich sichere Lösungsansätze wie die zentrale Vergabe bzw. Prüfung von Identitäten letztlich nur dann sicher sind, wenn auch die Vergabe sicher erfolgt. Ferner erscheint die Begrenzung der Sybil-Anzahl auf Basis der zur Verfügung stehenden IP-Adressen erfolgversprechend.

5.5 Ressourcenbasierte Analyse von Sybil-Angriffen

Der Zusammenhang zwischen Ressourcen wie Rechenleistung oder Bandbreite und dem resultierenden Einfluss eines Angreifers wurde bislang nicht vertieft un-

tersucht. Insofern ist es Ziel dieses Abschnitts, die möglichen Auswirkungen eines Sybil-Angriffs anhand einer ressourcenbasierten Analyse aufzuzeigen. Auf Basis der Analyse werden im Abschnitt 5.6 adäquate Abwehrstrategien entwickelt. Zunächst erfolgt eine Neubetrachtung der Definition von Douceur, woraus nochmals offensichtlich wird, dass die ressourcenbasierte Analyse von Sybil-Angriffen zielführend ist.

Douceurs Definition "Revisited": Legt man die ursprüngliche Definition von Douceur zugrunde, so handelt es sich um einen Sybil-Angriff, sobald es einer Entität gelingt, mit mehr als einer Identität im P2P-System zu agieren. Offen bleibt jedoch, was unter einer Entität verstanden wird und wie diese identifiziert wird.

Insbesondere bleibt dies auch bei der als Sybil-resistent geltenden zentralen Vergabe von Identitäten fraglich, da auch die zentrale Instanz Entitäten anhand eines kennzeichnenden Merkmals unterscheiden muss. Ein Exkurs zur Thematik "Identität in elektronischen Systemen" findet sich in Anhang B. In diesem werden nochmals explizit die Begriffe Entität und zugehörige Identität sowie deren Zusammenwirken diskutiert.

Selbst wenn Entitäten auf natürliche Personen zurückführt werden, kann sich ein Angreifer in der Regel mehrere Identitäten beschaffen, da die Prüfung der Identitäten wiederum von bestimmten Merkmalen abhängt. Werden hierzu bspw. CAPTCHAs[11] genutzt, kann ein Angreifer mehrere solche Tests bestehen und gegebenenfalls auch andere Nutzer durch monetäre Mittel dafür gewinnen, solche Tests zu lösen. Auch beim Einsatz anderer Merkmale wie Kreditkarte oder Pass stehen verschiedene Manipulationsmöglichkeiten offen. Der erforderliche Aufwand bzw. die nötigen Ressourcen eines Angreifers unterscheidet sich je nach Verfahren jedoch erheblich.

Da bei ganzheitlicher Betrachtung somit ein Sybil-Angriff immer möglich ist, bleibt letztlich fraglich, welchen Einfluss ein bestimmter Angreifer erlangen kann, genauer welches Verhältnis zwischen den zur Verfügung stehenden Ressourcen und dem möglichen Einfluss besteht. Insofern muss analysiert werden wie viele Ressourcen der Betrieb eines Knotens tatsächlich erfordert. Weiterhin müssen zur Quantifizierung des möglichen Einflusses eine Sybil-Metrik spezifiziert sowie entsprechende Analysen durchgeführt werden.

Evaluierungsmodell: Die ressourcenbasierte Analyse von Sybil-Angriffen erfordert:

[11] Der Ausdruck CAPTCHA steht für Completely Automated Public Turing Test to Tell Computers and Humans Apart und geht auf das gleichnamiges Projekt [WWW Captcha] zurück. Es handelt sich dabei um einen Test, um Menschen und Rechner zu unterscheiden, bei dem meist ein Bild mit verzerrtem Text genutzt wird [von Ahn et al. 2004].

1. die Bestimmung der Ressourcen, die ein Knoten verbraucht und
2. eine Untersuchung des Einflusses, den ein Angreifer mit einer bestimmten Menge an Ressourcen erzielen kann.

Die bisherige und folgende Betrachtungen des Sybil-Angriffs finden soweit möglich in allgemeiner, abstrahierter Form statt. Verschiedene Analysen, wie die Ermittlung des konkreten Ressourcenbedarfs eines Knotens und die Bestimmung des Einflusses von Sybils in den folgenden Abschnitten, erfordern jedoch eine Fokussierung auf ein konkretes P2P-Netz. Die aufgezeigte Methodik bleibt dabei ohne Weiteres auf andere P2P-Netze transformierbar.

Als konkretes P2P-Netz wurde für die Analysen Kademlia gewählt, da es einen hohen Verbreitungsgrad aufweist (vgl. Abschnitt 3.1.1). Analog wurde zur Bestimmung des Ressourcenverbrauchs in einer realweltlichen Umgebung die BitTorrent-DHT gewählt, die auf Kademlia basiert. Weitere Details zum Messaufbau und den Simulationsszenarien werden in den jeweiligen Abschnitten erläutert.

5.5.1 Ressourcenbasierte Analyse in der BitTorrent-DHT

Ein Sybil-Angriff erfordert auf Seiten des Angreifers gewisse IT-Ressourcen wie Netzwerkkapazitäten, Rechenleistung und Speicher. Um die Gefahr beurteilen zu können, bleibt insofern fraglich, wie viele Ressourcen durch ein Knoten konsumiert werden. Zur Messung wurde aus Gründen der Verbreitung und klaren Protokollspezifikation wie in Abschnitt 4.2.4 die BitTorrent-DHT gewählt.

Bislang existiert keine solche Untersuchung, da bekannte Messreihen andere Faktoren wie die Lebenszeit von Knoten (vgl. hierzu auch Abschnitt 4.2.4) oder die Dauer des Herunterladens einer Datei (vgl. u.a. [Izal et al. 2004]) fokussieren. Dies ist dadurch bedingt, dass der Datenverkehr, welcher durch die DHT verursacht wird, im Vergleich zum Herunterladen einer Datei vernachlässigbar ist. Für Gnutella existieren Arbeiten wie [Ripeanu 2001] oder [Pavlov & Saeed 2004], in welchen die benötigte Bandbreite für Suchnachrichten untersucht wird, da der Anteil an der Gesamtbandbreite bei Gnutella wesentlich höher ist. Eine Ausnahme bildet (in Teilen) die Arbeit [Qiao & Bustamante 2006], in welcher die Netzbandbreite von Kademlia-Knoten bestimmt wurde und die in der abschließenden Bewertung Berücksichtigung findet. Ferner wurde weder in den genannten Arbeiten noch bei Arbeiten zu Crypto-Puzzles die benötigte Rechenleistung oder der nötige Arbeitsspeicher analysiert.

Messergebnisse

Ziel der Messungen war es, folgende Ressourcenverbräuche zu bestimmen, die durch den Betrieb eines Knotens in der BitTorrent-DHT entstehen, ohne dass

dieser Knoten selbst aktiv nach Inhalten sucht:

- Netzlast durch ein- und ausgehende Datenpakete
- Auslastung der CPU
- Größe des benötigten Arbeitsspeichers

Messaufbau: Es gibt verschiedene P2P-Anwendungen, welche das BitTorrent-DHT-Protokoll gemäß der Spezifikation [BitT BEP5 2008] implementieren. Hierzu zählt insbesondere der so genannte Mainline-Client [WWW BitTorrent] und *libtorrent* [WWW libTorrent b]. Für die Messungen wurde eine angepasste Version von libtorrent verwendet, da es als Bibliothek realisiert ist und sich durch einen geringen Ressourcenverbrauch auszeichnet. So entfallen insbesondere alle graphischen Bedienelemente. Für die Messläufe 1 und 2 kam die Version 0.11 von libtorrent zum Einsatz. Dem 3. Messlauf lag eine angepasste Version von libtorrent Version 0.13 zugrunde. Außerdem konnte durch die Modifikation von libtorrent der Speicherverbrauch gesenkt, wie im Folgenden gezeigt wird.

Der erzeugte Netzwerkverkehr wurde mittels Wireshark [WWW Wireshark] aufgezeichnet. Die Interpretation und Filterung des Verkehrs erfolgte mittels eines eigens entwickelten Wireshark Dissectors[12]. Die Messungen der CPU-Auslastung und des Speicherverbrauchs basieren auf dem Unix-Werkzeug *ps*.

Für die Messungen wurde ein Rechner im Netz der Universität Karlsruhe (TH) betrieben, wobei die Ethernet-Anbindung 100 Mbit/s betrug. Als Rechner kam ein System auf Basis von Linux mit einer Dual-Core CPU vom Typ Intel Core2 T7200 zum Einsatz, die mit einer Taktfrequenz von 2,00 GHz betrieben wurde. Ferner verfügt der Rechner über 2 GByte Arbeitsspeicher.

Messergebnisse – Netzlast: Die Messungen wurden zu unterschiedlichen Zeitpunkten im Jahr 2007 und 2008, wie in Tabelle 5.1 aufgelistet, durchgeführt. Die Anzahl der Knoten gibt an, wie viele Knoten, genau genommen Sybils, parallel auf dem Messrechner betrieben wurden. Durch Testläufe im Vorfeld konnte gezeigt werden, dass der parallele Betrieb von mehreren Knoten unproblematisch ist.

Die Messknoten verhielten sich komplett protokollkonform. Die initiierten Suchanfragen nach Schlüsseln dienten lediglich dazu die Kademlia-Buckets zu befüllen bzw. aktuell zu halten. Des Weiteren wird von den Messknoten, wie im Protokoll vorgesehen, die Verfügbarkeit von bekannten Knoten durch eine Kademlia-Ping-Nachricht überprüft. Der restliche Datenverkehr ist bedingt durch die Anfragen anderer Knoten.

[12] Die Interpretation der Datenpakete erfolgt in Wireshark mittels so genannter Dissectors. Unbekannte Protokolle können durch Implementierung eines solchen Dissectors ergänzt werden.

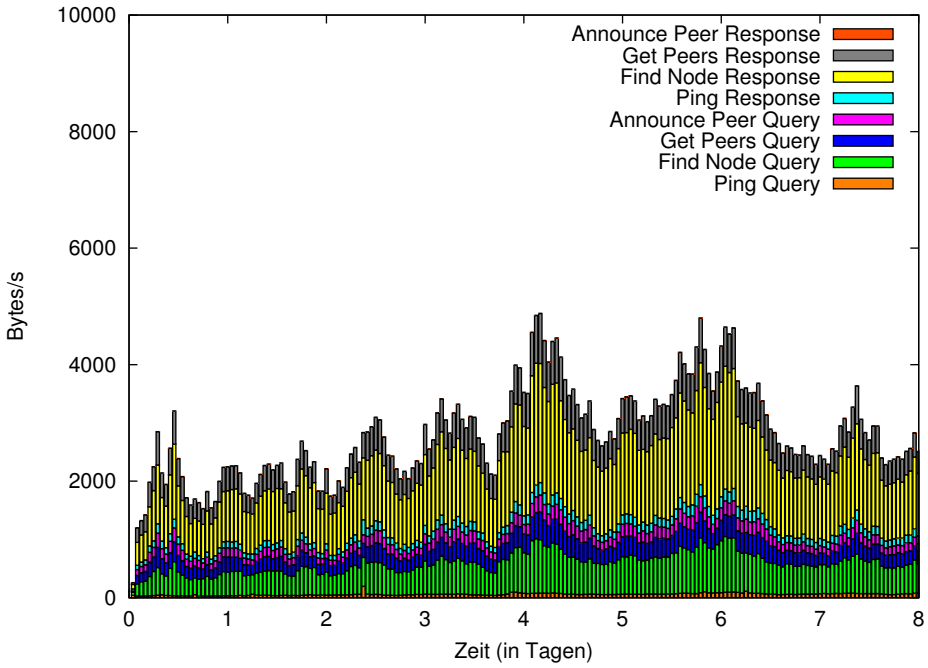


Abbildung 5.9: Aufschlüsselung des Datenverkehrs eines BitTorrent-DHT-Knotens nach Pakettypen

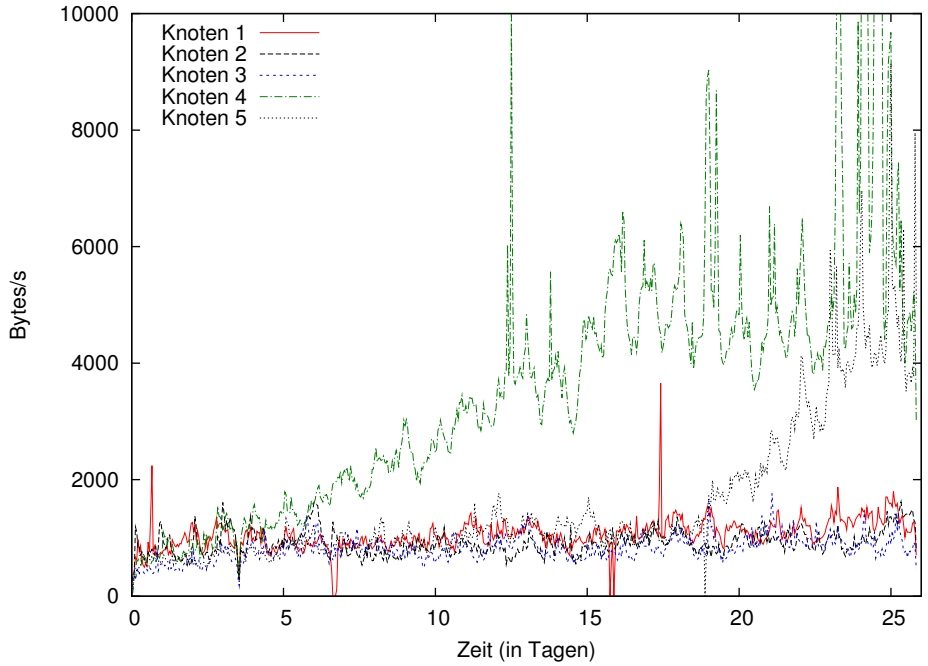


Abbildung 5.10: Netzlast durch eingehende Datenpakete beim ersten Messlauf je Knoten

	Dauer	Zeitraum	Knoten
1. Messlauf[1]	27 Tage	April 2007	5
2. Messlauf	8 Tage	Mai 2007	5
3. Messlauf	26 Tage	April 2008	5

[1] Ohne CPU- & RAM-Messungen

Tabelle 5.1: Übersicht der Messläufe zum Ressourcenverbrauch von Knoten in der BitTorrent-DHT

Abb. 5.9 zeigt exemplarisch eine Aufschlüsselung des Datenverkehrs nach Pakettypen entsprechend dem Knoten 1 aus dem 2. Messlauf. Dabei wird deutlich, dass der größte Anteil durch `Find_Node`-Anfragen und -Antworten sowie `Get_Peers`-Nachrichten bedingt ist[13]. Ein sehr geringer Anteil des Datenverkehrs geht auf `Announce_Peer`-Nachrichten zurück, d.h. der Knoten ist hauptsächlich mit dem Routing befasst und nur für wenige Schlüssel verantwortlich. Wie sich im Folgenden noch zeigt, ist daher der Speicherverbrauch konstant. Der hohe Anteil von `Find_Node`-Nachrichten resultiert daraus, dass diese häufig bei der Wartung der Routing-Tabelle genutzt werden.

In der Abb. 5.9 wird anhand der Antwortpakete deutlich, dass das Datenvolumen durch die Antwortpakete wesentlich höher als das der Anfragen ist. Dies ist auf die Tatsache zurückzuführen, dass eine Anfrage (im Wesentlichen) lediglich den gesuchten Schlüssel enthält, während bei der Antwort eine Liste von Knoten zurück gesendet wird.

Aus den Messungen wird auch deutlich, dass sich das Datenvolumen je Knoten deutlich unterscheidet. In Abb. 5.10 ist hierzu die benötigte eingehende Bandbreite je Knoten für den Messlauf 1 aufgetragen. Der unterschiedliche Bandbreitenbedarf ergibt sich aus der Tatsache, dass die Knoten verschiedene Knotenkennungen haben und somit für unterschiedliche Bereiche im Schlüsselraum zuständig sind. Da manche Schlüssel öfters angefragt werden wie andere, ergibt sich eine Differenz in der benötigten Bandbreite. Der durchschnittliche Bandbreitenbedarf schwankt dabei zwischen ca. 3.500 Bytes/s und 800 Bytes/s.

Weiterhin wurde aus den Messdaten der durchschnittliche Bandbreitenbedarf eines Knotens bei den Messläufen 1 und 3 bestimmt, der in Abb. 5.11 für eingehende und in Abb. 5.12 für ausgehende Verbindungen dargestellt ist. Der erhöhte

[13] Durch eine `Find_Node`-Anfrage wird der für einen Schlüssel zuständige Knoten bestimmt. `Get_Peers`-Nachrichten dienen hingegen dazu, den Wert zu einem Schlüssel (im Falle der BitTorrent-DHT eine Liste von Knoten, die eine Datei bereitstellen) zu ermitteln. Ist ein Knoten nicht für einen Schlüssel zuständig, wird auf beide Anfragen mit einer Liste von Knoten geantwortet, die näher zum gesuchten Schlüssel sind. Mittels `Announce_Peer`-Nachrichten wird ein Wert in der DHT eingetragen und `Ping`-Nachrichten dienen dazu die Erreichbarkeit zu überprüfen. Weitere Ausführungen finden sich in [BitT BEP5 2008].

Bandbreitenbedarf im dritten Messlauf ergab sich durch einen Knoten, der sehr stark frequentiert war. Die zeitliche Steigerung des Bandbreitenbedarfs ist durch das Kademlia-Protokoll bedingt, das langlebige Knoten bevorzugt. Der durchschnittliche Bandbreitenbedarf je Knoten und Messlauf ist in Tabelle 5.2 zusammengefasst.

Messergebnisse – CPU & RAM: Neben der benötigten Netzwerkbandbreite wurde auch die CPU-Last sowie der benötigte Arbeitsspeicher bestimmt.

Bei den Messungen zeigte sich, dass der Speicherverbrauch über die Laufzeit der Messungen, d.h. mehrere Tage und Wochen, in etwa konstant blieb. Bei den Messläufen 1 und 2, in welchen ein nicht optimierte Version von libtorrent zum Einsatz kam, betrug der Speicherverbrauch ca. 4,4 MByte pro Knoten. Beim dritten Messlauf kam eine optimierte Version zum Einsatz, mit welcher der Speicherbedarf um ca. 50 % gesenkt werden konnte (vgl. Tabelle 5.2). Bei der Speicheroptimierung wurde die Funktionalität von libtorrent auf die DHT-Funktionen reduziert. Es wurden insbesondere die Funktionen zum Herunterladen und Bereitstellen von Dateien, d.h. die ursprünglichen Grundfunktionen von BitTorrent, entfernt, da diese für den Betrieb der DHT nicht benötigt werden.

Die Messung der CPU-Auslastung beziehen sich auf die oben genannte CPU. Es zeigte sich, dass die Auslastung je Knoten sehr gering sind. Die CPU-Last betrug im zweiten Messlauf zwischen 0,06 % und 0,28 % je Knoten und zwischen 0,01 % und 0,49 % je Knoten im dritten Messlauf, was durchschnittlichen Werten von 0,13 % bzw. 0,16 % entspricht. Dabei bleibt zu beachten, dass ein Knoten bei Messlauf 3 sehr stark nachgefragt wurde.

Bewertung

Insgesamt zeigen die Messungen, dass der Ressourcenverbrauch im Wesentlichen durch die benötigte ausgehende Netzwerkbandbreite bestimmt ist. Die Auslastung der CPU und der Speicherverbrauch durch einen Knoten sind gering. Außerdem besteht dort noch Optimierungspotential, wie durch die optimierte Version von libtorrent gezeigt werden konnte. Bei der Netzwerkbandbreite besteht allerdings wenig Optimierungspotential, da Knoten, welche Suchanfragen nicht oder nur teilweise beantworten, von anderen Knoten weniger berücksichtigt werden; somit würde der Einfluss der Sybils beschränkt. In Tabelle 5.2 sind die Messergebnisse nochmals zusammengefasst.

Von weiteren Optimierungen hinsichtlich CPU-Last und Arbeitsspeicherverbrauch wurde abgesehen, da die Netzwerkbandbreite limitierend ist. So können auf einem aktuellen Rechner mit mehreren Gigabyte Arbeitsspeicher aus Sicht des Arbeitsspeichers mehrere tausend Knoten betrieben werden. Auch die Re-

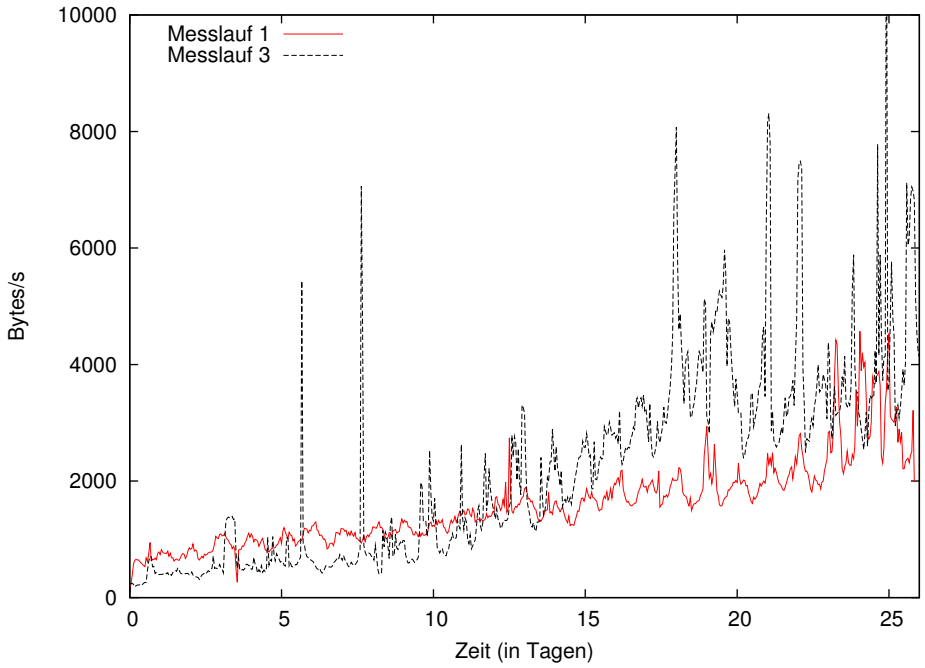


Abbildung 5.11: Durchschnittlicher Bandbreitenbedarf für eingehende Datenpakete bei den Messläufen 1 und 3

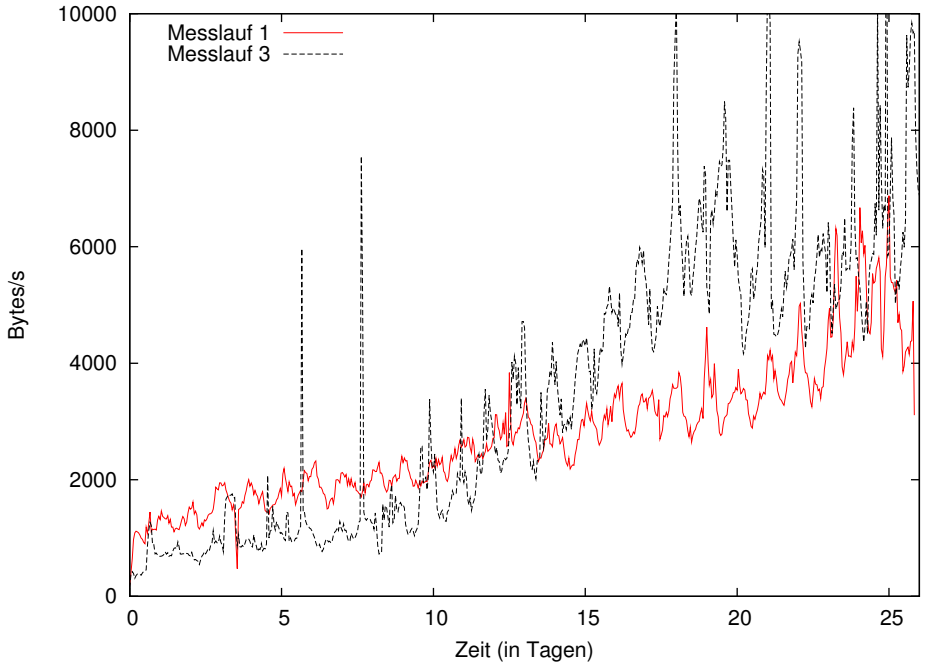


Abbildung 5.12: Durchschnittlicher Bandbreitenbedarf für ausgehende Datenpakete bei den Messläufen 1 und 3

	Netzlast eingehend	Netzlast ausgehend	CPU-Last	RAM
1. Messlauf	1.586 Bytes/s	2.758 Bytes/s	—	—
2. Messlauf	1.472 Bytes/s	2.526 Bytes/s	0,13 %	4,4 MByte
3. Messlauf	2.290 Bytes/s	3.573 Bytes/s	0,16 %	2,4 MByte

Tabelle 5.2: Durchschnittlicher Ressourcenverbrauch je Knoten und Messlauf

chenleistung aktueller CPUs lässt bereits ohne Optimierung den Betrieb mehrerer hundert bis tausend Knoten zu. Durch empirische Tests konnte dies auch nachvollzogen werden. So wurden auf einem Rechner problemlos 1.000 Knoten gleichzeitig betrieben.

Die Netzbandbreite ist jedoch nicht zu vernachlässigen, wobei vor allem die ausgehende Bandbreite der beschränkende Faktor ist. So bedarf es für den Betrieb von 1.000 Knoten einer Upstream-Bandbreite von ca. 2,9 MByte/s, was 23 MBit/s entspricht.

Darüber hinaus bleibt zu beachten, dass die notwendige Netzbandbreite protokollseitig beeinflusst werden kann, wenn das Aktualisierungsintervall zur Wartung der Routing-Tabelle erhöht oder reduziert wird. Die BitTorrent-DHT sieht hierfür ein Intervall von 15 Minuten vor. In [Qiao & Bustamante 2006] wird das entsprechende Intervall bei OverNet mit 30 Minuten angegeben. Die Autoren geben dann einen Wert von 100 bis 180 Byte/s für "Control Messages" eines Knotens an, wobei unklar bleibt, was in "Control Messages" enthalten ist[14]. Insofern sind die Ergebnisse aus [Qiao & Bustamante 2006] nur unzureichend vergleichbar.

5.5.2 Einfluss von Sybils

Um die Gefahr, welche von Sybils ausgeht, einschätzen zu können, ist neben der Analyse im vorigen Abschnitt auch ein Verständnis darüber nötig, welchen Einfluss ein Angreifer mit einem bestimmten Anteil von Sybils erlangen kann. Um den Einfluss zu quantifizieren, wird daher zunächst eine Metrik definiert. Sybil-Angriffe werden anschließend analysiert, wobei die Angriffe auch mit weiteren sekundären Angriffsmethoden wie dem Routing-Table-Poisoning kombiniert werden. Die Analysen dazu wurden simulativ durchgeführt.

[14] Der Text lässt darauf schließen, dass keine `Find_Node`-Nachrichten enthalten sind, die einen erheblichen Teil der Nachrichten ausmachen. Außerdem handelt es sich um eine andere DHT-Implementierung.

Sybil-Metrik

Ziel eines Sybil-Angriffs ist es, die Basis für die primären Angriffsmethoden zu schaffen (vgl. Abschnitt 5.3.1). Entscheidend ist insbesondere der Anteil bösartiger Knoten in den Routing-Tabellen der gutartigen Knoten. Je höher dieser Anteil ist, desto wahrscheinlicher ist es dass ein Sybil kontaktiert wird und der Angreifer somit sein Angriffsziel verfolgen kann. Dabei ist es unerheblich, ob ein Angreifer eine Störung, Überwachung oder Kontrolle zum Ziel hat. Insofern kann dies auch als Maßgabe für die Beurteilung des Erfolgs eines Sybil-Angriffs dienen und die folgende Metrik definiert werden:

> *Anteil bösartiger Routing-Tabelleneinträge* p_{malRTE}: Die Routing-Tabelleneinträge, welche auf bösartige Knoten verweisen, werden als *bösartige Routing-Tabelleneinträge* bezeichnet. Für die Berechnung der Metrik werden dabei nur die Routing-Tabelleneinträge von gutartigen Knoten berücksichtigt.

Simulationsszenarien

Für die Simulationen wurde der diskrete ereignisorientierte Netzwerksimulator OMNeT++ Version 3.4b2 [WWW OMNet] in Verbindung mit einer modifizierten Version der P2P-Erweiterung OverSim (Basisversion: SVN-Snapshot vom 20. Juli 2008) [WWW OverSim] verwendet. Als unterliegendes Netz wurde ein vereinfachtes IP-Netz genutzt, welches im Wesentlichen nur Bandbreitenrestriktionen aufweist.

Für den Beitritt zum P2P-Netz wird bei den Simulationen ein zufälliger aktiver Knoten und kein Bootstrap-Server genutzt. Soweit dies nicht anders kenntlich gemacht wurde, haben alle (sowohl gutartige als auch bösartige) Knoten eine beschränkte Lebenszeit – kurz aktivierter Churn. Wenn nicht anders angegeben, wurden für die Simulationsszenarien die Konfigurationsparameter gewählt, wie sie in Tabelle 5.3 angegeben sind. Zu beachten bleibt, dass die Anzahl gutarti-

P2P-Netz	Kademlia
Anzahl gutartiger Knoten	1.000
Aktualisierungsintervall der DHT	900 Sekunden[1]
Durchschnittliche Lebenszeit von Knoten	10.000 Sekunden[2]
Simulationsläufe pro Parametersatz	10
Simulationsdauer	600.000 Sekunden

[1] entspricht der Spezifikation der BitTorrent-DHT [BitT BEP5 2008]
[2] die Lebenszeit ist Pareto-verteilt entsprechend [Yao et al. 2006]

Tabelle 5.3: Konfigurationsparameter der Simulationsszenarien

ger Knoten konstant bleibt, um eine Vergleichbarkeit der Ergebnisse zu gewährleisten. Das Aktualisierungsintervall wird im Folgenden auch als "Ping-Rate" bezeichnet, da im Wesentlichen die Erreichbarkeit von Knoten überprüft wird (vgl. auch Abschnitt 2.4.3).

Für die Berechnung von Durchschnittswerten wurde der stabile Zustand (engl. Steady State) zum Zeitpunkt 600.000 Sekunden genutzt. Bei den dargestellten Konfidenzintervallen handelt es sich um 95 %-Konfidenzintervalle.

Analyse des Einflusses von Sybils mittels Simulationsstudie

Bei der Analyse des Einflusses von Sybils wurde ein Sybil-Angriff für sich sowie in Kombination mit Routing-Table-Poisoning und mit Churn untersucht.

Sybil-Angriff: Verhält sich der Angreifer "protokollkonform", d.h. er betreibt die Sybils wie normale Knoten, so entspricht erwartungsgemäß der Anteil bösartiger Routing-Tabelleneinträge dem Anteil bösartiger Knoten. In der zusammenfassenden Abb. 5.17 wird dies in der Kurve "ohne RTP, Churn bei allen Knoten" verdeutlicht.

Sybil-Angriff & Routing-Table-Poisoning: Der Einfluss von Sybils kann durch Routing-Table-Poisoning (RTP) erheblich gesteigert werden. Der Angriff wurde dabei wie folgt implementiert: Bösartige Knoten verweisen gutartige Knoten immer auf bösartige. Kommunizieren zwei bösartige Knoten miteinander, werden jedoch auch Routing-Informationen zu gutartigen Knoten ausgetauscht. Würden von den bösartigen Knoten nur bösartige Routing-Informationen ausgetauscht, käme es zu einer Separierung der bösartigen Knoten. Wie in ersten Implementierungen des Angriffs erkennbar war, führt dies zu einem deutlichen Rückgang der bösartiger Routing-Tabelleneinträge und ist aus Sicht des Angreifers daher kontraproduktiv. Bei dem Angriff wurde angenommen, dass sich alle bösartigen Knoten kennen und gutartige Knoten keine Möglichkeiten zur Verfügung stehen, den Angriff zu erkennen.

Durch die Verbreitung bösartiger Routing-Tabelleneinträge kann ein Angreifer seinen Einfluss in einem P2P-Netz erheblich erhöhen, wie die folgenden Ergebnisse zeigen. Der Einfluss nimmt dabei nach und nach zu, da auch gutartige Knoten diese Routing-Informationen weiterverbreiten. Abb. 5.13 zeigt den Anteil bösartiger Routing-Tabelleneinträge im zeitlichen Verlauf. Dabei wird insbesondere deutlich, dass bereits ein sehr geringer Anteil bösartiger Knoten ausreicht, um große Teile des P2P-Netzes zu dominieren. So kann ein Angreifer mit 10 % bösartiger Knoten nach 90 Stunden mehr als 60 % der Routing-Tabelleneinträge bestimmen. Abb. 5.13 zeigt aber auch, dass bei einem geringen Anteil bösartiger

Knoten, der Einfluss durch RTP nur wenig gesteigert werden kann. Im zweiten Fall sind oft bereits gutartige Knoten bekannt, die eine "nähere" Knotenkennung aufweisen als die bösartigen Knoten, so dass ein Großteil der bösartigen Routing-Informationen letztlich ignoriert wird.

Wie in der Abb. 5.13 deutlich wird, steigt der Anteil bösartiger Einträge zu Beginn stark an und im Anschluss nur noch langsam. Für die zusammenfassende Darstellung der Ergebnisse in Abb. 5.17, bei welcher auf der x-Achse der Anteil bösartiger Knoten aufgetragen ist, wurde daher der Durchschnittswert zum Zeitpunkt 600.000 Sekunden gewählt.

In Abb. 5.13 sind Durchschnittswerte angegeben. Der Anteil bösartiger Routing-Tabelleneinträge bei einzelnen Knoten ist jedoch unterschiedlich. Abb. 5.14 gibt diese Verteilung wieder, wobei zum Vergleich auch zwei Verteilungen ohne Routing-Table-Poisoning angegeben sind. Dabei wird deutlich, dass der Anteil Knoten, deren Routing-Tabelle vollständig mit bösartigen Einträgen besetzt ist, dem Anteil bösartiger Knoten entspricht. Dies ist dadurch bedingt, dass für das Bootstrapping ein zufälliger Knoten ausgewählt wird und ein Knoten gegebenenfalls nie mit einem anderen gutartigen Knoten in Kontakt kommt. Dies zeigt aber auch, dass durch Routing-Table-Poisoning alleine in der Regel keine vollständige Dominierung von Knoten möglich ist.

Aus den Ergebnissen ergibt sich, dass mittels RTP bösartige Knoten einen großen Einfluss im P2P-Netz ausüben können. Unberücksichtigt blieb bisher allerdings, dass bösartige Knoten ein erhöhtes Nachrichtenaufkommen bewältigen müssen, da sie in mehr Routing-Tabellen präsent sind und somit regelmäßig im Zuge der Wartung der Routing-Tabelle von mehr Knoten kontaktiert werden. Abb. 5.15 zeigt die notwendige ausgehende Bandbreite (engl. Upstream Bandwidth) je Angreifer, um den auf der x-Achse verzeichneten Anteil von Routing-Tabelleneinträgen in einem Netz mit 1000 Knoten zu beherrschen. Daraus ergibt sich unter anderem, dass 5 % bösartige Knoten erwartungsgemäß zu einem ca. 50-fach höheren Datenvolumen führen, da 5% der Knoten 52 Knoten entsprechen. Insgesamt zeigt sich, dass der Aufwand für einen Angreifer mit RTP jedoch wesentlich geringer als ohne. Die Ergebnisse für die eingehende Bandbreite sind analog.

Sybil-Angriff & Churn: Der aufgezeigte Effekt beim Routing-Table-Poisoning kann noch gesteigert werden, wenn es dem Angreifer gelingt, seine Knoten länger als gutartige Knoten zu betreiben. Dies ist dadurch bedingt, dass Kademlia langlebige Knoten beim Routing bevorzugt. Abb. 5.16 zeigt hierzu, wie sich der Anteil bösartiger Routing-Tabelleneinträge entwickelt, wenn die Lebenszeit der gutartigen Knoten wie zuvor begrenzt ist und die bösartigen Knoten eine unbegrenzte

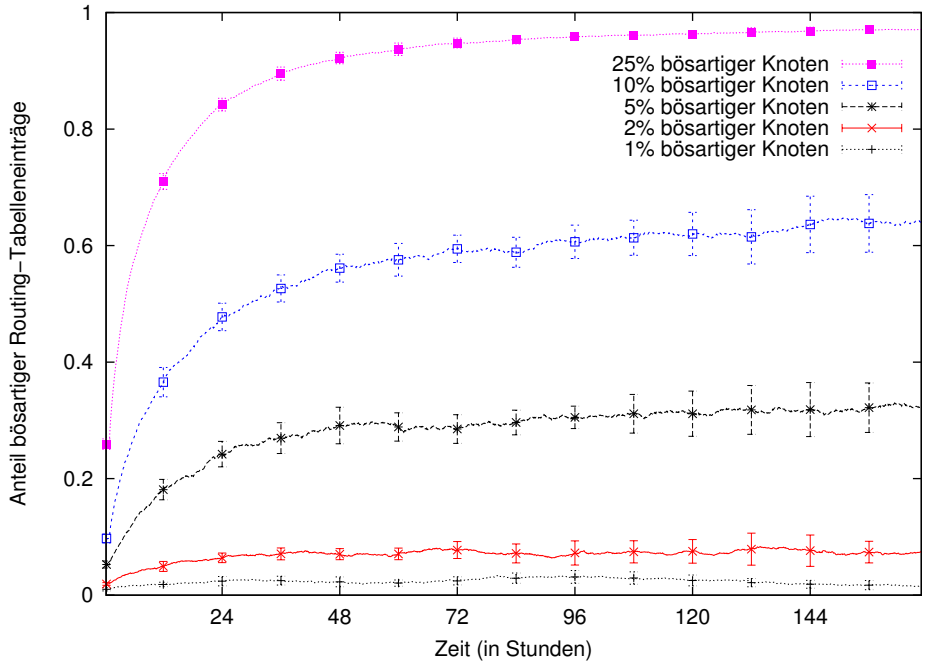


Abbildung 5.13: Zeitliche Entwicklung der bösartigen Routing-Tabelleneinträge unter dem Einfluss von Routing-Table-Poisoning (RTP)

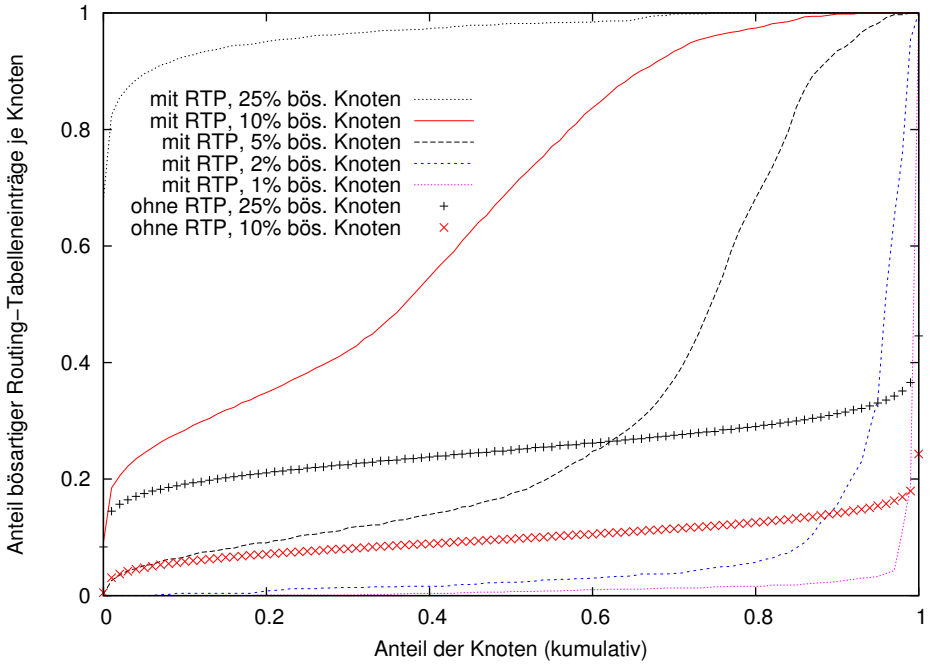


Abbildung 5.14: Anteil bösartiger Routing-Tabelleneinträge je Knoten mit und ohne Routing-Table-Poisoning (RTP), Anteil der Knoten ist kumulativ, d.h. x % der Knoten weisen maximal y % bösartige Routing-Tabelleneinträge auf

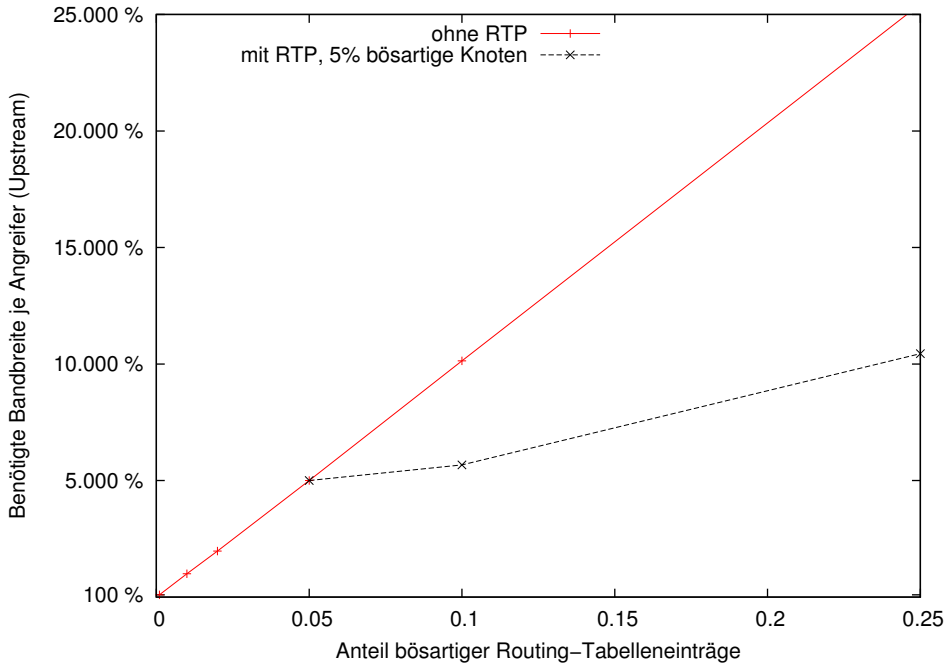


Abbildung 5.15: Effizienz des Routing-Table-Poisoning (RTP) bzgl. der ausgehenden Netzbandbreite im Vergleich zu einem "reinen" Sybil-Angriff (ohne RTP entspricht der Anteil bös. Knoten dem Anteil bös. Routing-Tab.)

Lebenszeit haben. So zeigt sich, dass 10 % bösartige Knoten über eine Laufzeit von 135 Stunden zu mehr als 20 % bösartiger Routing-Tabelleneinträgen führen. Ein Churn-Angriff ist insofern nicht zielführend, um den Einfluss von Sybils in einem P2P-Netz zu steigern. Vielmehr kann "künstliches Churn" dazu genutzt werden, den Einfluss von Sybils einzudämmen, wie in Abschnitt 5.6.3 dargelegt wird.

Bewertung

Die Ergebnisse zeigen, dass der Einfluss von Sybils durch Routing-Table-Poisoning deutlich gesteigert werden kann. So lassen sich mittels einem Anteil von 10 % bösartiger Knoten in einem Netz mehr als 60 % der Routing-Tabelleneinträge beherrschen. Andrerseits zeigte sich auch, dass bei einem sehr geringen Anteil bösartiger Knoten Routing-Table-Poisoning nur wenig Zugewinn hinsichtlich des Anteils bösartiger Routing-Tabelleneinträge verspricht, was insbesondere vorteilhaft für sehr große Netze mit Millionen von Knoten ist. Ferner kann der Angreifer seinen Anteil noch weiter erhöhen, wenn seine Knoten langlebiger als die gutartigen Knoten sind. In Abb. 5.17 sind die Ergebnisse zusammengefasst dargestellt.

Die abschließende Ressourcenverbrauchsanalyse zeigt aber auch, dass die notwendigen Ressourcen auch beim RTP nicht zu vernachlässigen sind, da bösarti-

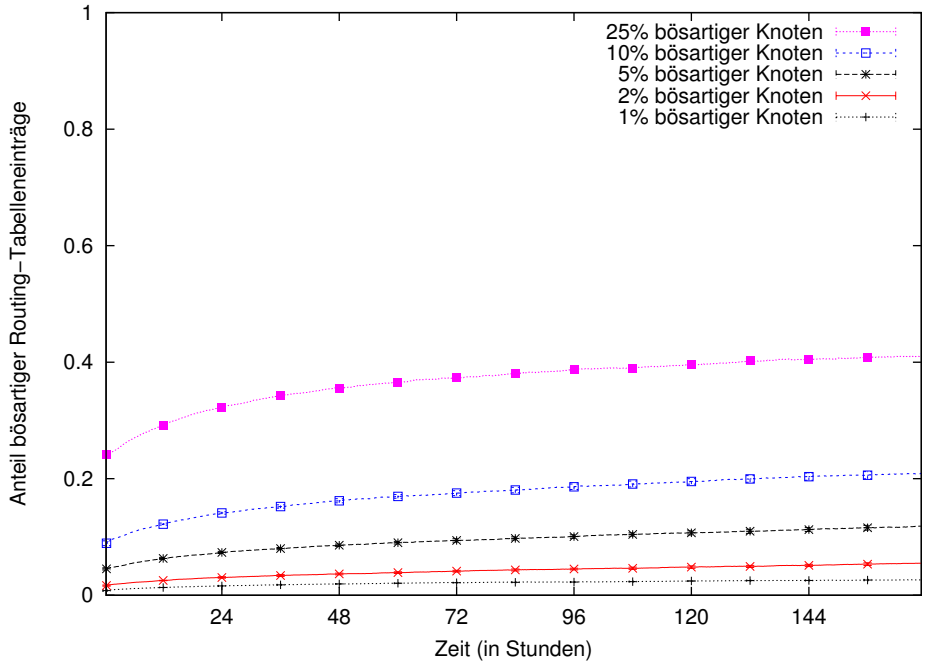


Abbildung 5.16: Auswirkung von Churn auf den Anteil bösartiger Routing-Tabelleneinträge, bei einer unbegrenzten Lebenszeit bösartiger Knoten (ohne Routing-Table-Poisoning)

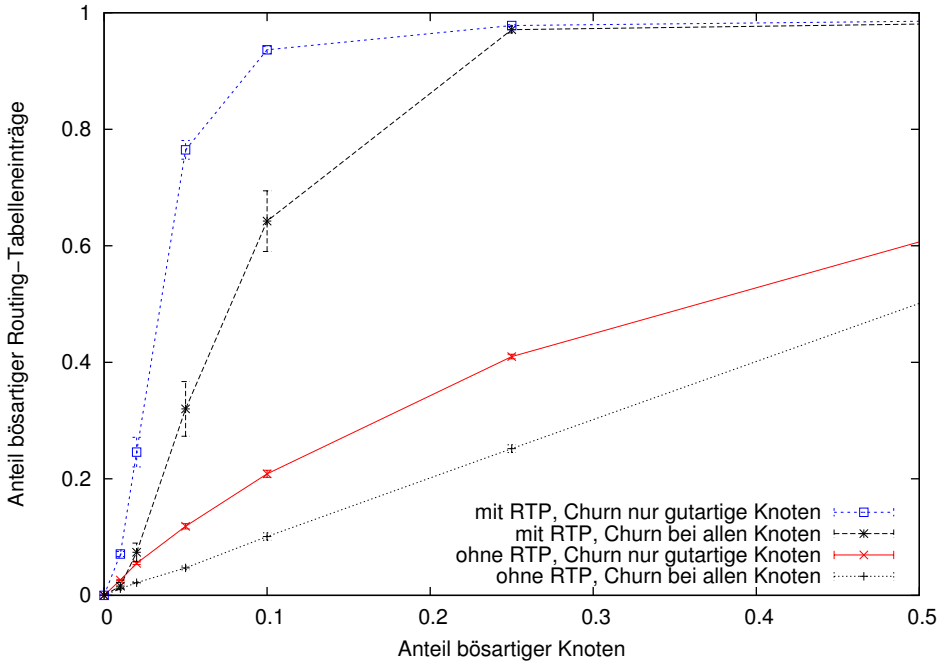


Abbildung 5.17: Verhältnis zwischen dem Anteil bösartiger Knoten und dem Anteil bösartiger Routing-Tabelleneinträge mit und ohne Routing-Table-Poisoning (RTP)

ge Knoten durch die hohe Präsenz in den Routing-Tabellen ein erhöhtes Nachrichtenaufkommen bewältigen müssen. Weiterhin bleibt zu beachten, dass ein RTP eine gewisse Anzahl Sybils voraussetzt, da ein bösartiger Knoten nur einmal in der Routing-Tabelle eines gutartigen Knotens vorkommt. Somit ist RTP zum einen durch die notwendigen Ressourcen begrenzt. Zum anderen kann RTP durch Techniken, wie eine strikte Routing-Tabelle (vgl. [Castro et al. 2002a] und [Hildrum & Kubiatowicz 2007]), eingeschränkt werden (vgl. Abschnitt 5.3.3).

5.5.3 Resümee

In diesem Abschnitt wurden zwei Aspekte betrachtet zum einen die Frage, wie viele Ressourcen für den Betrieb eines BitTorrent-DHT-Knotens notwendig sind, und zum anderen wurde aufgezeigt, welchen Einfluss Sybils ausüben können.

Aus umfangreichen realweltlichen Messungen in der BitTorrent-DHT geht hervor, dass die Ressourcen insbesondere die nötige Upstream-Bandbreite für den Betrieb von einigen tausend Knoten beträchtlich sind. So benötigt bereits *ein* BitTorrent-DHT-Knoten eine durchschnittliche ausgehende Netzbandbreite von ca. 24 kbit/s. Im Vergleich dazu sind die CPU-Auslastung und der Arbeitsspeicherverbrauch zu vernachlässigen.

Bei der Untersuchung des Einflusses von Sybils ergab sich, dass sich der Anteil bösartiger Routing-Tabelleneinträge linear zum Anteil der Sybils verhält, wenn keine weiteren Manipulationen vorgenommen werden. Wird Routing-Table-Poisoning eingesetzt, steigt der Anteil jedoch überproportional an, wenn die "Grundlage" bösartiger Knoten groß genug ist (größer 2 % bösartiger Knoten). In beiden Fällen erhöht sich das Datenvolumen beträchtlich, wobei Routing-Table-Poisoning aus Sicht des Angreifers dennoch deutlich effizienter ist.

Insgesamt zeigt sich, dass eine nicht zu vernachlässigende Gefahr von Sybil-Angriffen ausgeht, der Angreifer besonders bei großen Netzen jedoch beträchtliche Ressourcen aufwenden muss. Im folgenden Abschnitt werden auf Basis dieser Erkenntnisse ressourcenbasierte Abwehrstrategien entwickelt.

5.6 Verfahren zur Erhöhung der Sybil-Resistenz

Aus den vorigen Abschnitten geht hervor, dass ein vollständiger Schutz gegen einen Sybil-Angriff bei ganzheitlicher Betrachtung unter realen Umgebungsbedingungen nicht möglich ist. Vielmehr soll durch Abwehrmechanismen die Generierung von Sybils erschwert werden, so dass deren Einfluss gering bleibt. In den vorigen Abschnitten wurden hierzu mögliche limitierende Faktoren ermittelt.

Der Fokus dieser Arbeit liegt dabei nicht auf Verfahren, die ergänzende Dienste oder zusätzliches Wissen erfordern, wie es bei einer zentralen Kennungsvergabe oder beim Einbezug sozialer Netze der Fall ist. Vielmehr ist Gegenstand der Untersuchung, inwieweit die Anzahl der Sybils auf Basis der zur Verfügung stehenden Ressourcen und Identifikationsmerkmale beschränkt werden kann.

Da eine Ressourcenbeschränkung nicht in jedem Fall zielführend ist, bleibt fraglich ob die IP-Adresse als zusätzliches Element genutzt werden kann, um die Anzahl Sybils pro Angreifer zu begrenzen. Die IP-Adresse stellt dabei keine Ressource im eigentlichen Sinne dar, da sie vielmehr ein Identifikationsmerkmal auf Netzwerkebene ist. Andererseits kann ein Angreifer über mehrere IP-Adressen verfügen, so dass keine 1-zu-1 Beziehung zwischen IP-Adresse und Angreifer mehr gegeben ist. In einem erweiterten Kontext können IP-Adressen somit auch als eine Art Ressource verstanden werden (vgl. insofern auch Anhang B). Aus Gründen der besseren Lesbarkeit bezieht sich der Begriff Ressourcen im Folgenden nach wie vor auf die "klassischen" Ressourcen Netzbandbreite, Rechenleistung, Speichergröße und nicht IP-Adressen.

Zunächst wird die Limitierung der Sybil-Anzahl auf Basis der Ressourcen diskutiert. Im Abschnitt 5.6.2 wird anschließend ein neuartiges so genanntes Selbstregistrierungsverfahren vorgestellt wird, mittels dessen die Knotenanzahl pro IP-Adresse bzw. -Adressbereich effektiv beschränkt werden kann. Ergänzend wird ein Verfahren zum Knotenaustausch, so genannter künstlicher Churn, skizziert mittels dessen vollständig dominierte Knoten sich aus ihrer Isolation lösen können und der Einfluss des Routing-Table-Poisoning begrenzt wird. Abschließend wird die Anwendbarkeit der dargelegten Abwehrmechanismen am Beispiel zweier typischer Angreifertypen aufgezeigt. Den Simulationen liegt die Szenariodefinition gemäß Abschnitt 5.5.2 zugrunde.

5.6.1 Ressourcenbasierte Limitierung

Wie in Abschnitt 5.5 gezeigt, benötigt der Betrieb vieler Sybils in einem realen Netz durchaus eine beträchtliche Ressourcenmenge. Insofern ergibt sich daraus die Möglichkeit, eine ressourcenbasierte Limitierung von Sybils einzuführen.

Ausgestaltung der Ressourcenprüfung: Bei der Überprüfung der Ressourcen muss die Abwägung zwischen einem akzeptablen Ressourcenbedarf für gutartige Knoten und der Effektivität zur Verhinderung eines Sybil-Angriffs getroffen werden. So wäre es nicht wünschenswert, dass ein durchschnittlicher Nutzer mit einer CPU-Auslastung von 50 % rechnen muss.

Eine Überprüfung der Ressourcen muss in regelmäßigen Abständen stattfinden, da ein Angreifer ansonsten frei werdende Ressourcen für die Erzeugung wei-

terer Knoten nutzen kann [Douceur 2002]. Die Überprüfung kann dabei explizit wie bei der Rechenleistung durch ein Crypto-Puzzles erfolgen oder implizit wie bei der Netzbandbreite, indem Knoten, die nicht rechtzeitig auf Anfragen antworten, aus der Routing-Tabelle entfernt werden.

Allen Verfahren zur Überprüfung gemein ist, dass die eingesetzten Ressourcen letztlich "vergeudet" werden, wobei bei der Netzbandbreite immerhin ein positiver Effekt hinsichtlich der Aktualität der Routing-Tabelle eintritt.

Eignung der Ressourcen: Als limitierende Ressourcen steht die Rechenleistung, der Speicherplatz sowie die Netzwerkbandbreite zur Auswahl.

Speicherplatz kann hinsichtlich Zugriffsgeschwindigkeit und verfügbaren Kapazitäten in verschiedene Speicherarten wie Arbeitsspeicher und Festplattenspeicher unterteilt werden. Für den Betrieb eines Knotens ist zwar eine gewisse Menge an Arbeitsspeicher nötig. Eine effektive Ressourcenbeschränkung auf Basis des Speicherplatzes erfordert jedoch die Verteilung und Speicherung von nicht komprimierbaren Daten. Die Dynamik eines P2P-Netzes würde keine vorige Verteilung zulassen, so dass die Daten zunächst übertragen werden müssten und somit die Netzbandbreite wieder limitierend wird. Insgesamt ist Speicherplatz daher ungeeignet, um eine Sybil-Resistenz durch Ressourcenbeschränkung in P2P-Netzen zu etablieren.

Die beiden Ressourcen Rechenleistung und Netzbandbreite können hinsichtlich der Ressourcenbeschränkung zusammengefasst betrachtet werden. Muss ein Knoten regelmäßig eine gewisse Anzahl CPU-Zyklen investieren, um bspw. ein Crypto-Puzzle wie in [Borisov 2006] zu lösen, so kann dies letztlich überführt werden in eine Anzahl an Nachrichten, die ein Knoten durchschnittlich in einer bestimmten Zeit bearbeiten kann.

Ebenso lässt sich die Netzbandbreite als limitierende Ressource nutzen, indem die Ping-Rate erhöht wird, d.h. die Rate mit welcher an bekannte Knoten "Pings" versendet werden und von denen dann jeweils eine Antwort erwartet wird. Beantwortet ein Knoten Anfragen nicht, wird er aus den Routing-Tabellen entfernt. Augenfällig dabei ist, dass die Netzbandbreite die Anzahl der Nachrichten beschränkt, die in einem Zeitintervall empfangen bzw. versendet werden können und somit die Limitierung auf die gleiche Metrik zurückgeführt werden kann. Insofern werden die Beschränkungen im Folgenden durch Erhöhung der Ping-Rate und Limitierung der Netzbandbreite aufgezeigt.

Aus folgenden Gründen erscheint die Überprüfung der Rechenleistung jedoch ohnehin nicht zielführend zu sein. Die Leistungssteigerung bei Prozessoren ist exponentiell (vgl. u.a. [Meuer 2008]) und somit eine Limitierung nur in beschränktem Maße möglich ist. Die Netzbandbreite steigt zwar auch, aber in der Regel in

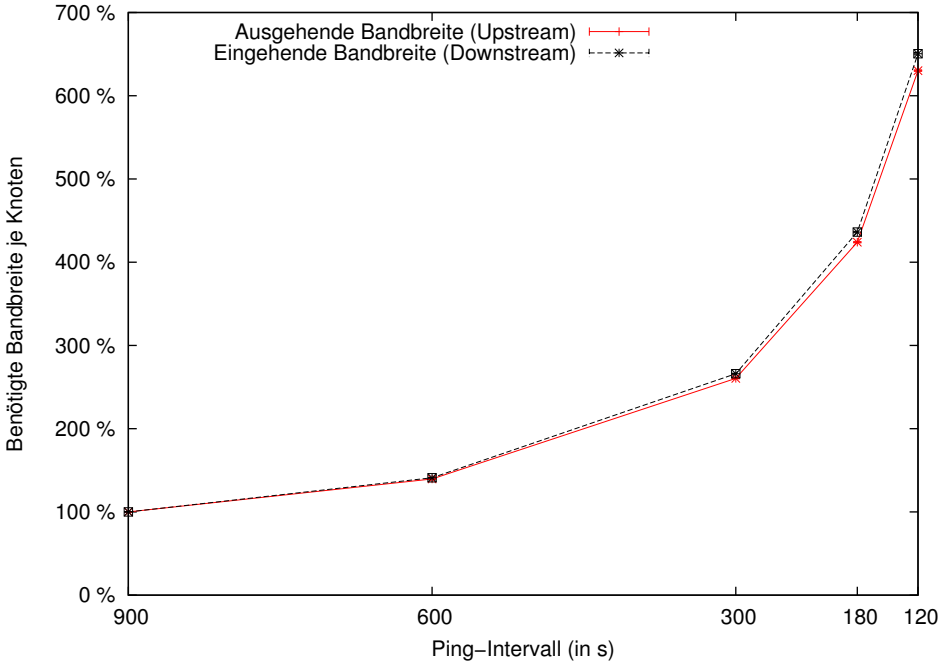


Abbildung 5.18: Verhältnis zwischen Ping-Rate und Nachrichtenaufkommen pro Knoten

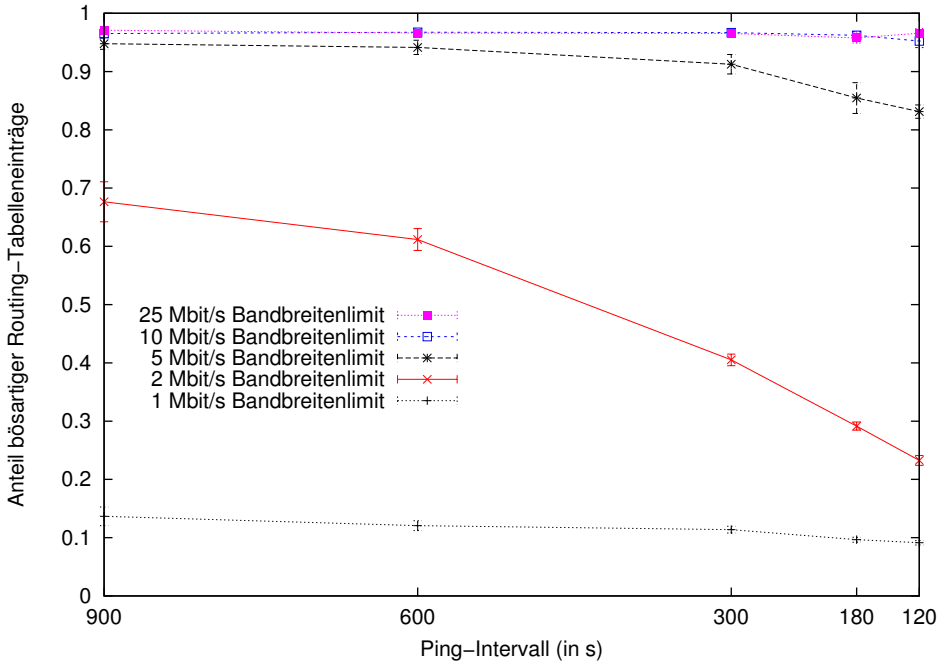


Abbildung 5.19: Schwindender Einfluss eines Angreifers durch Erhöhung der Ping-Rate bei 1.000 gutartigen und 25 % bösartigen Knoten mit RTP und Bandbreitenlimit (Hinweis: Bandbreitenbedarf eines Knotens entsprechend Simulation)

geringerem Maße als die Rechenleistung. Erschwerend kommt hinzu, dass Knoten teilweise in leistungsschwachen Geräten wie NAT-Routern integriert sind, die nur über eine sehr geringe Rechenleistung verfügen. Insofern ist zu erwarten, dass das Verhältnis zwischen der minimal zur Verfügung stehenden Rechenleistung und der Rechenleistung eines Angreifers in der Regel wesentlich größer ist, als bei der zur Verfügung stehenden Netzbandbreite.

Auch die Messergebnisse aus Abschnitt 5.5.1 weisen in diese Richtung, da die CPU-Auslastung im Vergleich zur Netzlast wesentlich geringer ist und die Überprüfung der Rechenleistung somit wesentlich mehr Ressourcen verschwenden würde.

Ein Vorteil der Limitierung auf Netzebene ist weiterhin, dass ein Angreifer diese Ressourcen ständig selbst vorhalten muss, während bei der Überprüfung der Rechenleistung die Berechnung gegebenenfalls ausgelagert werden kann. Es bietet sich daher an die Netzbandbreite als limitierende Ressource zu nutzen.

In Abb. 5.18 wird für ein Kademlia-Netz aufgezeigt, wie sich die Anzahl der Nachrichten und somit die benötigte Bandbreite pro Knoten erhöht, wenn die Ping-Rate gesteigert wird. Dabei zeigt sich, dass die benötigte Bandbreite bei halbierter Ping-Rate doppelt so hoch ist.

Um die Effektivität der Limitierung der Sybils zu zeigen, wurde die Bandbreite des Angreifers begrenzt und der Einfluss bei unterschiedlichen Ping-Raten untersucht. Dem Angreifer stehen dabei 333 bösartige Knoten zur Verfügung, was einem Anteil von 25 % entspricht und er nutzt zusätzlich Routing-Table-Poisoning. In Abb. 5.19 ist ersichtlich, dass bei abnehmender Bandbreite und erhöhter Ping-Rate der Einfluss eines Angreifers deutlich limitiert ist. Dabei ist zu beachten, dass die Bandbreitenbedarf eines Knotens in der Simulation nicht exakt der realweltlichen Messung der BitTorrent-DHT entspricht, da die BitTorrent-DHT unter anderem eine Datenkodierung verwendet, die ein größeres Datenvolumen erzeugt.

Bewertung: Insgesamt zeigt sich, dass eine Limitierung der Sybils auf Basis der verfügbaren Ressourcen effektiv möglich ist.

Nachteilig bei einer ressourcenbasierten Limitierung ist jedoch, dass die verfügbaren Ressourcen stetig zunehmen, so dass Annahmen über Ressourcen, die einem Teilnehmer minimal zur Verfügung stehen, und die Ressourcen des Angreifers stetig angepasst werden müssen. Eine solche Anpassung wäre bspw. im Zuge von neuen Software-Releases durchführbar.

Weiterhin bleibt zu beachten, dass die Spanne der zur Verfügung stehenden Ressourcen sehr groß sein kann, wobei aus oben genannten Gründen die Netzbandbreite noch am geeignetsten ist, um eine Limitierung zu realisieren. Die vielfach diskutierte Überprüfung der Rechenleistung durch Crypto-Puzzles zeichnet

sich hingegen nicht als zielführend ab.

Fragwürdig bei allen Verfahren zur Ressourcenprüfung bleibt jedoch, dass in Summe eine große Menge an Ressourcen belegt ist und somit letztlich auch vergeudet wird. Dies ist umso bedenklicher, da es ursprünglich das Ziel von P2P-Systemen war, brachliegende Ressourcen nutzbar zu machen (vgl. Abschnitt 3.3.3) und eine Ressourcenprüfung in diesem Sinne eher kontraproduktiv ist. Darüber hinaus ist eine solche Ressourcenverschwendung und das zunehmende Interesse an energieeffizienten Systemen zuwiderlaufend, da für den Betrieb der Ressourcen und somit die Überprüfung der Ressourcen nicht unerheblich viel Energie aufgewendet werden muss.

5.6.2 Das Selbstregistrierungsverfahren

Neben der "klassischen" Ressourcenbeschränkung steht bei Knoten im Internet in Form der IP-Adresse ein weiteres Merkmal zur Verfügung, welches gegebenenfalls zur Limitierung der Sybils Verwendung finden kann. Bereits in [Stoica et al. 2001] wurde die Ableitung der Knotenkennung aus der IP-Adresse mittels einer konsistenten Hash-Funktion wie SHA-1 vorgesehen. Dem Verfahren liegt dabei die Annahme zugrunde, dass ein Angreifer nur über eine IP-Adresse verfügt.

Nachteilig bei dem genannten Verfahren ist, dass jeweils nur ein Knoten unter einer IP-Adresse betrieben werden kann, was insbesondere beim Einsatz von NAT-Routern zu Einschränkungen führt. Auch in Hinblick auf IPv6 erweist sich die Nutzung der kompletten IP-Adresse als wenig zielgerichtet, da ein Angreifer die letzten 64 bit der Adresse in der Regel selbst bestimmen kann (vgl. [RFC 4291, Sec. 2.5.4][15]. Ferner führen einige Autoren (vgl. u.a. [Yu et al. 2006] oder [Douceur 2002]) an, dass IP-Adressen manipuliert (engl. IP-Address Spoofing) werden können.

Trotz der Möglichkeit IP-Adressen zu fälschen, ist es im Internet nicht ohne Weiteres möglich, mittels einer solchen gefälschten IP-Adresse zu kommunizieren. Das Versenden von Datenpaketen unter einer gefälschten IP-Adresse ist zwar teilweise möglich[16]. Spätestens der Empfang von Datenpaketen, die an eine andere beliebige IP-Adresse adressiert sind, ist dennoch kaum möglich[17]. Insofern wird im Folgenden angenommen, dass ein Knoten im Besitz einer IP-Adresse ist, wenn er von dieser Datenpakete versenden und empfangen kann.

Ziel ist es daher, ein Verfahren zu entwickeln, mittels dessen die Anzahl Sybils

[15] Aus Datenschutzgründen ist das regelmäßige Wechseln der IP-Adresse durch verändern der letzten 64 bit sogar wünschenswert (vgl. [RFC 4941]).

[16] Außerdem setzen viele ISPs die Filterregeln aus [RFC 2827] um und überprüfen daher beim Versenden von Datenpaketen aus dem eigenen Netzbereich, ob es sich um legitime IP-Adressen handelt und verwerfen IP-Pakete mit gefälschten Absenderadressen.

[17] Dies trifft nicht auf IP-Adressen im gleichen Subnetz zu.

pro IP-Adresse bzw. Adressbereich unter Berücksichtigung der genannten Defizite bekannter Verfahren effektiv beschränkt werden kann. So sollte es insbesondere möglich sein, mehrere Knoten mit der gleichen IP-Adresse zu betreiben.

Lösungsansatz: Selbstregistrierung

Der Begriff *Registrierung* wurde übernommen von Verfahren mit zentraler Vergabe von Knotenkennung, bei welchen sich die Knoten registrieren, um eine Knotenkennung zu erhalten[18].

Der Kerngedanke des Selbstregistrierungsverfahrens besteht darin, dass sich die Knoten im P2P-Netz *selbst registrieren* und andere Knoten die korrekte Registrierung verifizieren können. Die Anzahl der Registrierungen pro IP-Adresse ist dabei limitiert und im Unterschied zu bekannten Verfahren kann hierbei auf zentralisierte Registrierungsstellen verzichtet werden.

Um am P2P-Netz teilnehmen zu können, muss ein Knoten eine Knotenkennung $\mathtt{nodeId}$ entsprechend folgender Vorschrift berechnen und dafür eine passende Registrierungskennung $\mathtt{regId}$ wählen[19]:

$$\mathtt{nodeId} := \mathrm{h}(\mathtt{ipAddr} \oplus \mathtt{regId}) \tag{5.7}$$

Die Variable $\mathtt{ipAddr}$ entspricht der IP-Adresse oder einem IP-Adresspräfix der IP-Adresse des Knotens, der sich registrieren will (vgl. hierzu auch den Abschnitt Parametrisierung). Im Folgenden wird soweit möglich der zusammenfassende Ausdruck IP-Adressbereich für $\mathtt{ipAddr}$ gebraucht.

Für die Registrierungskennung gilt $\mathtt{regId} \in \{1, \ldots, \mathtt{regId}_{max}\}$. Die maximale Anzahl Sybils pro IP-Adressbereich kann dabei durch die $\mathtt{regId}_{max}$ parametrisiert werden. Knoten, deren IP-Adressbereich gleich ist, benötigen eine unterschiedliche Registrierungskennung, da ansonsten zwei Knoten die gleiche Knotenkennung hätten.

Zwei Fragen blieben bislang jedoch offen: Zum einen, wie die Auswahl der $\mathtt{regId}$ erfolgt, und zum anderen was passiert, wenn keine freien Registrierungskennungen mehr vorhanden sind.

Routing-aktive und Routing-passive Knoten: Sowohl für die Phase, in welcher eine noch freie Registrierungskennung ermittelt wird, als auch für den Fall, dass alle belegt sind, ist eine Unterscheidung zwischen Routing-aktiven und Routing-passiven Knoten zielführend.

[18] vgl. auch Registrierungsstelle (engl. Registration Authority, RA) bei PKIs

[19] Aus Gründen der besseren Lesbarkeit und der wenigen mathematischen Terme wurden an dieser Stelle mehrere Zeichen zur Auszeichnung der Elemente verwendet.

Bei Routing-aktiven Knoten handelt es sich um reguläre Knoten eines P2P-Netzes. Routing-passive Knoten hingegen sind zwar protokollkonform, werden aber nicht in die Routing-Tabellen der anderen Knoten aufgenommen. Ferner werden auch keine Schlüssel/Wert-Paare auf Routing-passiven Knoten abgelegt.

Insofern sind Routing-passive Knoten nicht in den Routing-Prozess involviert, außer sie starten selbst eine Anfrage. Den Routing-passiven Knoten ist es insbesondere möglich, das Routing des P2P-Netzes zu nutzen und Schlüssel abzufragen. Routing-passiven Knoten benötigen dafür auch nicht zwingend eine Knotenkennung, da hierfür die Netzwerkadresse ausreicht.

Um eine Unterscheidung von Routing-aktiven und -passiven Knoten zu ermöglichen, fügen die Routing-aktiven Knoten ihre Registrierungskennung und resultierende Knotenkennung den Nachrichten hinzu. In Verbindung mit der IP-Adresse, die sich aus dem Datenpaket selbst ermitteln lässt, kann somit durch andere Knoten die Registrierung verifiziert werden.

Wahl der Registrierungskennung: Ein Knoten ist in der Wahl seiner Registrierungskennung frei. Um eine freie zu ermitteln, berechnet ein Knoten hierzu mögliche Knotenkennungen gemäß der Formel (5.7) und überprüft im P2P-Netz jeweils, ob diese bereits von einem anderen Knoten verwendet werden. Solange ein Knoten eine freie Registrierungskennung sucht, handelt es sich um einen Routing-passiven Knoten.

Die Überprüfung der freien Registrierungskennungen stellt in der Regel kein Skalierungsproblem dar, da $\mathtt{regId}_{max}$ klein gewählt wird, um die Zahl der Sybils zu begrenzen und somit auch nicht viele potentielle Knotenkennungen überprüft werden müssen. Zur Effizienzsteigerung kann je IP-Adressbereich von einem bereits Routing-aktiven Knoten eine Liste bereits vergebener Registrierungskennungen gepflegt werden. Der zuständige Knoten berechnet sich durch Anwenden der Hash-Funktion auf den entsprechenden IP-Adressbereich $\mathtt{h(ipAddr)}$.

Erst wenn ein Knoten eine freie Registrierungskennung ermittelt hat, kann er diese in Datenpaketen beifügen und wird somit zum Routing-aktiven Knoten.

Werden bereits alle Registrierungskennungen von anderen Knoten genutzt, bleibt ein Knoten in der Rolle des Routing-passiven Knotens. In dieser Rolle kann er am P2P-Netz teilnehmen, er wird einzig nicht von anderen Knoten für das Routing oder die Ablage von Schlüssel/Wert-Paaren genutzt. Um den Kontakt mit Routing-aktiven Knoten aufrecht zu erhalten, wählen auch Routing-passive Knoten eine Knotenkennung, indem sie eine noch beliebige freie Registrierungskennung wählen, die größer als $\mathtt{regId}_{max}$ ist, und pflegen ihre eigene Routing-Tabelle dementsprechend. Somit verteilen sich die Routing-passiven Knoten gleichmäßig im P2P-Netz.

Verifikation der Knotenkennung: Die Verifikation, dass sich ein Knoten korrekt registriert hat, erfolgt, indem einerseits die IP-Adresse überprüft und andererseits die Berechnung der Knotenkennung verifiziert wird.

Zur Überprüfung einer IP-Adresse sendet der empfangende Knoten ein Ping-Paket (auf P2P-Ebene) an die Adresse des sendenden Knotens und erwartet wiederum ein Antwortpaket zurück. Dadurch kann sichergestellt werden, dass der sendende Knoten mittels dieser IP-Adresse Datenpakete versenden und empfangen kann und somit nach der obigen Annahme aktuell im Besitz dieser IP-Adresse ist. Wurde die IP-Adresse verifiziert, kann im zweiten Schritt die Knotenkennung mit der Formel (5.7) berechnet werden, da der Knoten seine Registrierungskennung im Datenteil der Nachricht mit sendet.

Ergibt sich daraus eine andere Knotenkennung, wird dieser Knoten nicht in die Routing-Tabelle aufgenommen und auch nicht für die Ablage von Schlüssel/Wert-Paaren genutzt. Ferner wird ein Knoten auch dann als Routing-passiv betrachtet, wenn seine Registrierungskennung größer als die maximal erlaubte ist.

Parametrisierung: Die Länge des IP-Adresspräfixes sollte bei dem Verfahren so gewählt werden, dass einerseits ein Angreifer unter gegebenen Rahmenbedingungen mit hoher Wahrscheinlichkeit nur wenige IP-Adressen besitzt und andererseits keine Beeinträchtigung für legitime Knoten entsteht. Für IPv4 wird daher die Verwendung der kompletten 32 bit IP-Adresse empfohlen, während bei IPv6 ein Präfix von 64 bit gewählt werden sollte[20]. Der Präfix kann grundsätzlich jedoch eine beliebige Länge aufweisen. Die Präfixlänge muss lediglich bei allen Knoten gleich sein.

Es sollte nicht das Ziel sein, mittels des IP-Adresspräfixes eine Verteilung der Knoten auf IP-Adressbereiche zu forcieren, da dies auch nicht der faktischen Verteilung von potentiellen Knotenbetreibern entspricht. So sind bspw. in Dial-Up-Netzen, wie in Abschnitt 4.2 gezeigt, mehr Knoten zu erwarten. Abb. 5.20 zeigt die Anzahl der BitTorrent-Knoten pro IP-Adressbereich bei einer Präfixlänge von 16 bit. Die Abbildung basiert auf den Adressdaten von mehr als 5 Millionen BitTorrent-DHT-Knoten, wobei jede IP-Adresse nur einfach gezählt wurde. Die Daten wurden im Rahmen der Messungen aus Abschnitt 4.2 gewonnen.

Die maximale Registrierungskennung sollte möglichst klein gewählt werden. Um zu ermitteln, wie viele Knoten in realen Netzen mit der gleichen IP-Adresse betrieben werden, müssten die IP-Adressen aller gerade aktiven Knoten (gleichzeitig) ermittelt werden. Dies gestaltet sich bei großen Netzen mit mehreren Mil-

[20] Die letztliche Festlegung der Anzahl zu berücksichtigender Bits ist bei IPv6 aus praktischer Sicht bislang kaum möglich, da IPv6 momentan nur wenig Verbreitung gefunden hat und somit typische Vorgehensweisen erst etablieren müssen.

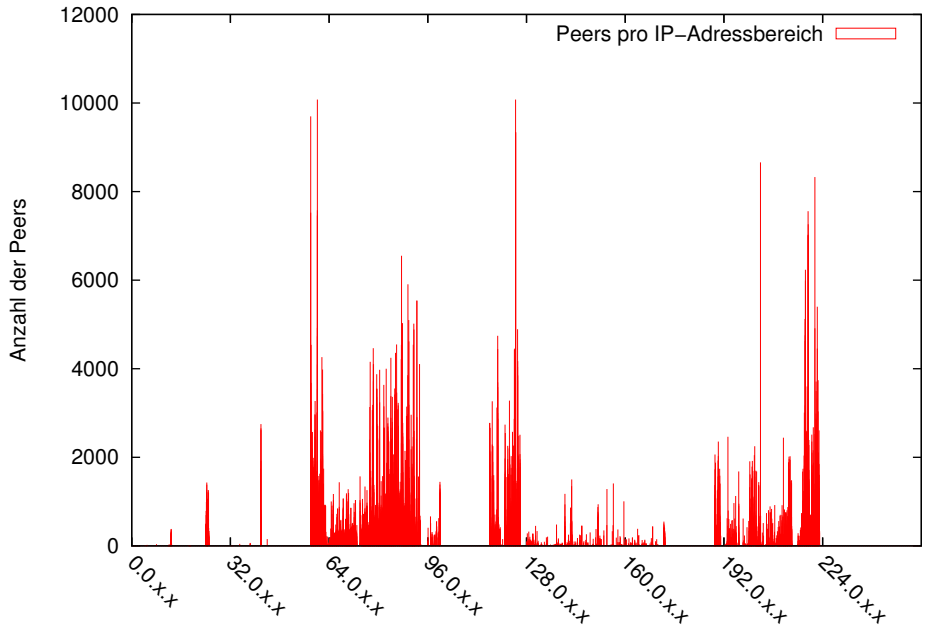


Abbildung 5.20: BitTorrent-DHT-Knoten je IP-Adressbereiche bei 16 bit Adresspräfix (Datenbasis: 5,2 Millionen Datensätze, vgl. Abschnitt 4.2.4)

lionen Knoten sehr schwierig. Insofern kann nur eine Abschätzung je nach Einsatzzweck erfolgen. Werden die freien Registrierungskennungen auf einem bereits aktiven Knoten verwaltet, wie oben zur Effizienzsteigerung erläutert, kann mittels dieser Daten auch eine Untersuchung der Knoten pro IP-Adressbereich in zukünftigen P2P-Netzen stattfinden.

Im Allgemeinen sollte jedoch eine $\mathrm{regId}_{max} < 5$ ausreichen. Im schlechtesten Falle kommt es dabei zu mehr Routing-passiven Knoten als nötig, was sich gegebenenfalls negativ auf die Skalierbarkeit des P2P-Netzes auswirken könnte. Eine Untersuchung der zusätzlichen Last, die durch Routing-passive Knoten entsteht, findet daher im Rahmen der Bewertung im folgenden Abschnitt statt.

Bewertung der Selbstregistrierung

In Zusammenschau mit den Prinzipien von Sit und Morris (vgl. Abschnitt 5.3.3) ergibt sich als Basis für möglichst Sybil-resistente Protokolle: i) Knotenkennungen sollten durch andere Knoten verifizierbar sein. ii) Die Anzahl der Knotenkennungen und somit Knoten pro Entität sollte möglichst gering sein.

Bei dem beschriebenen Selbstregistrierungsverfahren kann die Verifikation der Knotenkennung durch Berechnung des Terms (5.7) von anderen Knoten nachvollzogen werden. Sollten zwei Knoten die gleiche Registrierungskennung verwenden, führt dies zu inkonsistentem Routing-Verhalten. Aus dem Blickwinkel

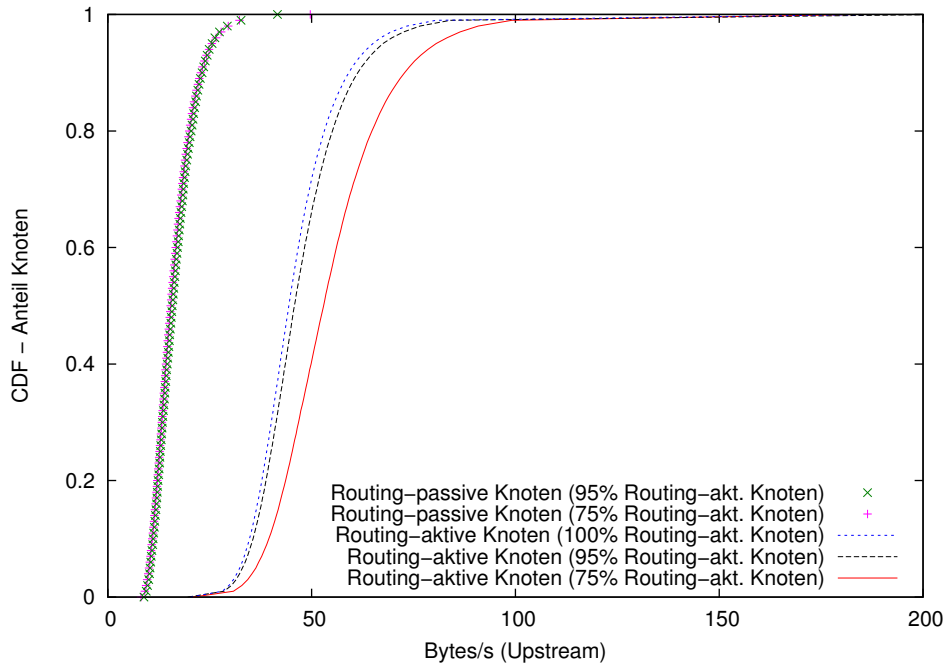


Abbildung 5.21: Ausgehende Netzlast für Routing-aktive und -passive Knoten bei einem variierenden Anteil Routing-aktiver Knoten

eines Sybil-Angriffs bleibt es jedoch bei einem Knoten, da *eine* Knotenkennung nicht mehrfach in die Routing-Tabellen anderer Knoten aufgenommen wird. Die Verifikation der Knotenkennung kann bei jedem Knoten lokal ohne den Einbezug von Informationen anderer Knoten stattfinden und ist somit unabhängig vom Anteil bösartiger Knoten im Netz.

Die Limitierung pro Entität ergibt sich durch die maximale Registrierungskennung $\mathtt{regId}_{max}$, durch welche die maximale Knotenanzahl pro IP-Adressbereich festgelegt wird. Dabei sei erwähnt, dass dieses Verfahren weder das Fälschen von IP-Adressen verhindert, noch dass ein Angreifer eine große Anzahl IP-Adressen besitzt. Das Selbstregistrierungsverfahren stellt jedoch effektiv sicher, dass die Anzahl der Sybils pro IP-Adresspräfix begrenzt bleibt, wobei sowohl das Limit als auch die Länge des Adresspräfixes beliebig parametrisierbar sind.

Durch Routing-passive Knoten entsteht eine zusätzliche Last für Routing-aktive Knoten. Da jedoch damit zu rechnen ist, dass die Anzahl der Routing-passiven Knoten insgesamt sehr gering ausfällt, ist diese Last in der Regel nur leicht erhöht. Abb. 5.21 zeigt die Erhöhung der benötigten Bandbreite pro Knoten bei Routing-aktiven Knoten. Daraus ergibt sich, dass bei einem Anteil von 95 % Routing-aktiver Knoten lediglich ein Overhead von ca. 3,2 % für Routing-aktive Knoten entsteht und selbst bei einem Anteil von 75 % Routing-aktiver Knoten beträgt der Overhead nur 19,8 %.

Der Anreiz sich als Routing-passiver Knoten auszugeben, obwohl noch Registrierungskennungen frei sind, ist gering, da das erzeugte Datenvolumen einer DHT beim Betrieb *eines* Knotens gering ist (ca. 24 kbit/s bei der BitTorrent-DHT). Insbesondere ist der Anreiz wesentlich geringer als beim Austausch von großen Dateien.

Ein positiver Nebeneffekt des Berechnungsverfahrens ist, dass ein Knoten seine Knotenkennung nicht selbst bestimmen kann und nur eine begrenzte Auswahl von Registrierungskennungen zur Verfügung steht, so dass auch eine Besetzung bestimmter Bereiche im P2P-Netz nahezu unmöglich ist.

5.6.3 Künstlicher Churn

Der Einfluss von Sybils kann durch Routing-Table-Poisoning wesentlich gesteigert werden. Die Effizienz der Angriffsmethode liegt darin begründet, dass auch gutartige Knoten bösartige Routing-Tabelleneinträge verbreiten.

Insofern ist es in diesem Falle zielführend Knoten in den Routing-Tabellen in regelmäßigen Abständen auszutauschen und somit die Auswirkungen des Routing-Table-Poisoning zu begrenzen und eine Rehabilitierung von vollständig isolierten Knoten zu ermöglichen. Dieser neuartige Mechanismus wird als "künstlicher Churn" bezeichnet.

Bei künstlichem Churn wird in regelmäßigen Abständen ein Teil der Knoten der Routing-Tabellen ausgetauscht, obwohl diese Knoten noch erreichbar sind. Die für den Austausch nötigen Knoten können dabei durch eine dezentrale Knotensuche, wie in Abschnitt 4.2.3 beschrieben, gewonnen werden. Inspiriert wurde das Verfahren durch die Arbeit [T. Condie et al. 2006], in welcher ein ähnliches Verfahren vorgestellt wird, wobei dort ein synchrones Zurücksetzen der Routing-Tabelle mittels einer zentralen Komponenten auf eine strikte Routing-Tabelle vorgesehen ist. Im Unterschied dazu funktioniert, dass in dieser Arbeit vorgeschlagene Verfahren vollständig dezentral.

In Abb. 5.22 ist die begrenzende Wirkung des künstlichen Churn exemplarisch dargestellt, wobei eine Anteil von 25 % bösartiger Knoten angenommen wurde und in den angegebenen Intervallen jeweils 3 Knoten ausgetauscht werden. Der Anstieg zu Beginn ist dadurch bedingt, dass der künstliche Churn Mechanismus erst nach 5 Stunden aktiviert wurde. Aus den Ergebnissen wird deutlich, dass bereits bei einem Austauschintervall von 600 Sekunden letztlich eine Reduktion der bösartigen Routing-Tabelleneinträge von 97 % auf 60 % erreicht werden kann.

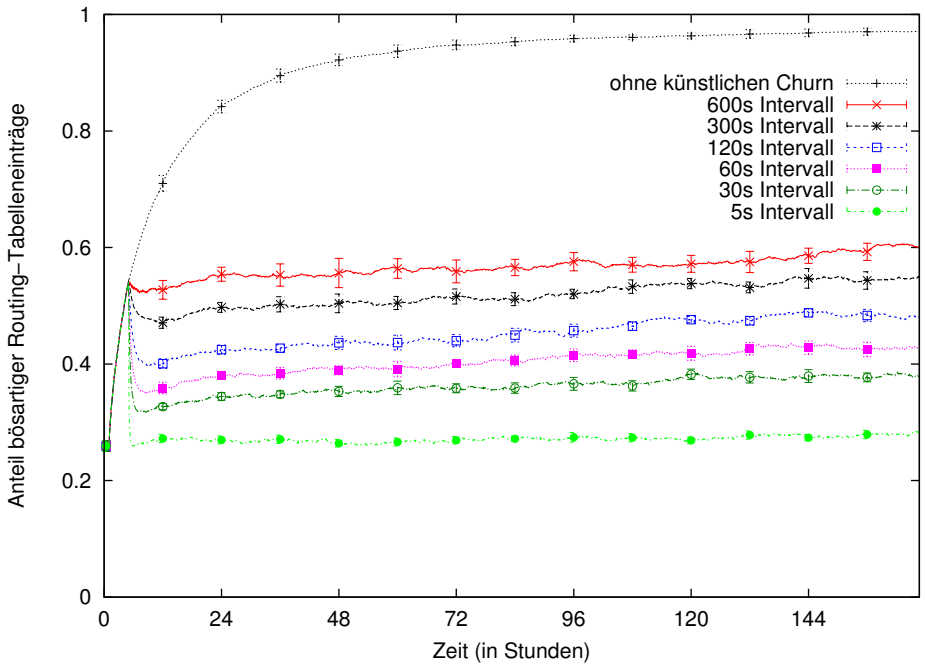


Abbildung 5.22: Begrenzung des Routing-Table-Poisoning durch den Einsatz von künstlichem Churn bei 25 % bösartiger Knoten

5.6.4 Resümee zur Sybil-Resistenz

Der abschließenden Betrachtung zur Sybil-Resistenz durch Ressourcenbeschränkung liegen zwei Angreifermodelle zugrunde, anhand derer die wesentlichen Ergebnisse der vorigen Abschnitte nochmals verdeutlicht werden. Weiterhin gelte die Annahme, dass ein Angreifer seinen Angriff möglichst kosteneffizient gestalten möchte (vgl. hierzu auch [Margolin & Levine 2008]).

Für die Angreifer werden dabei, wie in anderen Arbeiten (vgl. u.a. [Castro et al. 2002a] und [Yu et al. 2006]) auch, folgende Annahmen getroffen:

- **Angreifer A:** Dieser Angreifer verfüge über ein so genanntes Botnet, d.h. ein Netz von Rechnern, die mit einer Schadsoftware infiziert sind und von *einem* Angreifer gesteuert werden können.
- **Angreifer B:** Der zweite Angreifer sei ein bösartiger ISP (engl. rogue ISP), der im Besitz einer sehr großen Anzahl von IP-Adressen ist.

Botnets können aus mehreren tausend Rechnern bestehen [Rajab et al. 2007], die sich in der Regel in verschiedenen IP-Netzbereichen befinden. Nachteilig bei Botnets ist für einen Angreifer jedoch, dass die IP-Adressen nicht oder nur in einem sehr beschränkten Maße wählbar sind. Im Gegensatz dazu kann der Angreifer B seine IP-Adressen nahezu beliebig wählen. Dabei ist jedoch die verfüg-

bare Bandbreite geringer, da die kumulierte Bandbreite eines Botnets in der Regel günstiger ist, als die Bandbreite "am Stück" einzukaufen.

Im Folgenden wird dargelegt, für welchen Angreifertyp die klassische ressourcenbasierte Limitierung und für welchen das Selbstregistrierungsverfahren geeignet ist. Wie in Abschnitt 5.6.1 erläutert, ist eine Erhöhung der Netzlast zielführend, um die Ressourcen eines Knotens zu prüfen und wird daher im Weiteren fokussiert. Zudem wird zwischen zielgerichteten lokalen und globalen Angriffen entsprechend Abschnitt 5.3 unterschieden.

Botnets eignen sich für einen Sybil-Angriff bestens, da die Knoten im Botnet sehr schwer oder gar nicht von "normalen Knoten" zu unterscheiden sind. Insofern kann der Angreifer A mindestens so viele Knoten betreiben, wie sein Botnet Rechner enthält. Ziel sollte es jedoch sein, die Anzahl der Knoten pro Botnet-Rechner zu begrenzen, da somit auch die Kosten für den Angreifer steigen, der für den gleichen Angriff ein größeres Botnet benötigt.

Eine klassische ressourcenbasierte Limitierung auf Basis der Netzbandbreite oder gar Rechenleistung ist bei Angreifer A nicht erfolgversprechend, da die kumulierten Ressourcen im Botnet sehr groß sind oder andernfalls gutartige Knoten sehr viele Ressourcen investieren müssten. Die Beschränkung der Anzahl Sybils auf Basis der IP-Adresse ist hingegen zielführend, da diese Limitierung durch das Selbstregistrierungsverfahren effektiv realisierbar ist und die Anzahl Sybils pro Botnet-Rechner minimiert.

Da durch dieses Verfahren auch die Auswahl der Knotenkennung begrenzt wird, dient dieses Verfahren beim Angreifer A auch zur Abwehr von lokalen Angriffen. Dabei bleibt zu beachten, dass es dem Angreifer A je nach P2P-Netz möglich ist, Routing-Table-Poisoning zu betreiben und somit seinen Anteil zu erhöhen. Hierzu kann zusätzlich ein striktes Routing-Verfahren wie Chord (vgl. Abschnitt 5.3.3) oder künstlicher Churn in Erwägung gezogen werden. Außerdem ist Routing-Table-Poisoning nur bei einem großen Anteil bösartiger Knoten kritisch.

Sowohl bei Angreifer A als auch B ist eine ressourcenbasierte Limitierung durch die Netzlast nicht geeignet, um lokale Angriffe abzuwehren, da für lokale Angriffe nur wenige Ressourcen nötig sind. Um einen globalen Angriff des Angreifers B einzuschränken, ist eine Limitierung durch die Netzlast aber zielführend. Das Selbstregistrierungsverfahren kann seine Effektivität nicht entfalten, da der Angreifer B über viele IP-Adressen verfügt und somit die Annahme, die bei der Gestaltung des Verfahrens zugrunde gelegt wurde, nicht erfüllt ist.

In Tabelle 5.4 sind die Ergebnisse zusammengefasst. Daraus ergibt sich, dass sich die beiden Verfahren der Limitierung durch die Netzlast und das Selbstregistrierungsverfahren gut ergänzen, um P2P-Netze resistenter gegen Sybil-An-

	Globaler Angriff	**Lokaler Angriff**
Angreifer A	⊖ Limitierung durch Netzlast	⊖ Limitierung durch Netzlast
(Botnet)	⊕ Selbstregistrierung	⊕ Selbstregistrierung
Angreifer B	⊕ Limitierung durch Netzlast	⊖ Limitierung durch Netzlast
(rogue ISP)	⊖ Selbstregistrierung	⊖ Selbstregistrierung

Tabelle 5.4: Zusammenfassung der Eignung der Limitierung durch Netzlast und der Selbstregistrierung bei unterschiedlichen Angreifern

griffe zu machen.

Trotz der Effektivität der Verfahren kann ein Angreifer, der über genügend Ressourcen verfügt, die genannten Schutzmechanismen aushebeln. Unter der Annahme, dass eine 100 %-ige Sicherheit in realen Umgebungen ohnehin nicht möglich ist, kann durch die genannten Verfahren jedoch ein entscheidender Beitrag geleistet werden, um die Auswirkungen eines Sybil-Angriffs zu begrenzen.

Zusammenfassend lassen sich folgende Empfehlungen formulieren, um P2P-Netze unter Berücksichtigung der vorhandenen IT-Ressourcen Sybil-resistenter zu gestalten:

- Die Ressourcenüberprüfung sollte regelmäßig erfolgen, wobei die Prüfung direkt zwischen den Knoten stattfinden sollte.
- Die Knotenkennungen sollten entsprechend dem Selbstregistrierungsverfahrens generiert und verifiziert werden, um die Anzahl der Knoten pro IP-Adressbereich zu begrenzen.
- Die erforderlichen Ressourcen pro Knoten sollten in regelmäßigen Abständen angehoben werden, um die steigende Netzbandbreite bzw. Rechenleistung zu kompensieren.
- Durch künstlichen Churn kann die Sybil-Resistenz erhöht werden.

5.7 Zusammenfassung

In diesem Kapitel wurde die Robustheit von P2P-Systemen bzw. -Netzen aus zwei Blickwinkeln betrachtet. Einerseits erfolgte zunächst eine Betrachtung, die vom Aspekt der Fehlertoleranz getrieben war. Der zweite, überwiegende Teil des Kapitels widmete sich P2P-spezifischen Angriffen und insbesondere dem Sybil-Angriff, von welchem eine besonders große Gefahr für P2P-Netze ausgeht.

Insgesamt konnte mittels der präsentierten wahrscheinlichkeitstheoretischen Betrachtungen, den simulativen Analysen und der realweltlichen Messungen ein

umfassendes Bild der Robustheit von P2P-Netzen und insbesondere der Gefährdung durch Sybils gezeichnet werden. Dabei wurde bewusst auf die Spezifikation eines konkreten Anwendungsszenarios verzichtet. Vielmehr wird dem Leser die Möglichkeit eröffnet die Ergebnisse auf ein spezifisches Szenario anzuwenden, indem die nötigen Berechnungsmethoden dargelegt und mögliche Entwurfsentscheidungen diskutiert wurden. Insofern kann dieser Abschnitt als eine Art Leitfaden für die Entwicklung und den Betrieb eines P2P-Systems gebraucht werden. Darüber hinaus konnte die Sybil-Resistenz durch die entwickelten Verfahren Selbstregistrierung und künstlicher Churn maßgeblich gesteigert werden.

Die Analyse der Fehlertoleranz von P2P-Systemen ergab, dass Fail-Stop-Fehler sowohl beim Routing als auch bei der Datenhaltung ein untergeordnetes Problem darstellen und durch Redundanzmechanismen leicht handhabbar sind. Der Umgang mit byzantinischen Fehlern beim Routing erfordert jedoch schon ein beträchtliches Maß an Redundanz.

Durch P2P-spezifische Angriffe verschärft sich die Situation noch weiter. Um die bekannten Angriffe einzuordnen, wurde ein Einordnungsschema entwickelt, welches sich in Angriffsziele sowie primäre und sekundäre Angriffsmethoden gliedert. Dabei erwies sich der Sybil-Angriff als besonders schwerwiegend.

Daher wurden nachfolgend Grundlagen und bekannte Lösungsansätze zum Sybil-Angriff dargelegt und bewertet, wobei sich herausstellte, dass der Aspekt des Ressourcenbedarfs von Knoten bislang nur unzureichend betrachtet wurde. So blieb unter anderem unklar wie groß der erforderliche Bandbreitenbedarf eines Knotens ist.

Zunächst wurde daher mittels einer umfangreichen realweltlichen Messung über mehrere Wochen hinweg der Ressourcenverbrauch von Knoten in der BitTorrent-DHT ermittelt. Daraus ergab sich, dass vor allem die benötigte Upstream-Bandbreite mit durchschnittlich ca. 24 kbit/s maßgeblich ist.

Durch eine simulative Analyse wurde in der Folge gezeigt, welchen Einfluss ein Angreifer mittels Sybils ausüben kann. Dabei wurde auch deutlich, dass die Effektivität eines Sybil-Angriffs durch die Kombination mit Routing-Table-Poisoning wesentlich erhöht werden kann.

Generell zeigt sich, dass sich ein Sybil-Angriff bei ganzheitlicher Betrachtung und unter realistischen Annahmen, selbst bei der zentralen Vergabe von Identitäten, nicht unterbinden lässt. Ziel war es daher, den Einfluss und die Erzeugung von Sybils zu begrenzen bzw. die Kosten, welche einem Angreifer entstehen, in die Höhe zu treiben.

Daher wurde ein neuartiges Selbstregistrierungsverfahren entwickelt, mittels dessen sich die Anzahl der Sybils pro IP-Adresse effektiv beschränken lässt. Durch das entwickelte Verfahren kann somit vor allem der Einfluss von Botnets deutlich

begrenzt werden. Ferner konnte durch simulative Analysen gezeigt werden, dass die Skalierbarkeit beim Einsatz des Verfahrens gewährleistet bleibt.

Darüber hinaus wurde auch die Einsatzmöglichkeiten einer Beschränkung auf Basis der Netzlast und Rechenleistung untersucht. Hierbei erwies sich die Netzlast als geeigneter und effektiv nutzbar. Allerdings werden bei einer solchen Limitierung sehr viele Ressourcen verschwendet, was vor dem Hintergrund energieeffizienter Systeme und dem ursprünglichen Ziel von P2P-Systemen, brachliegende Ressourcen zu nutzen fragwürdig erscheint. Abschließend konnte in Simulationsexperimenten gezeigt werden, dass die Nutzung von künstlichem Churn, d.h. der regelmäßige Austausch von Knoten der Routing-Tabelle, eine erhöhte Sybil-Resistenz bei Routing-Table-Poisoning erlaubt.

6

Telekommunikationsrechtliche Einordnung

In diesem Kapitel wird eine Einordnung von P2P-Systemen und -Netzen in den telekommunikationsrechtlichen Rahmen vorgenommen. Dabei findet sowohl die nationale als auch die europäische Gesetzgebung Berücksichtigung. Im ersten Teil des Kapitels wird basierend auf einer umfassenden Analyse hierfür ein neuartiges Einordnungsschema entwickelt, indem insbesondere die juristischen Bewertungsmaßstäbe in Einklang mit fachwissenschaftlichen Aspekten der Informatik gebracht werden. Anhand des gewonnen Einordnungsschema werden in weiteren Abschnitten die resultierenden Rechtsfolgen sowie die Voraussetzungen und Folgen des Eingreifens von telemedienrechtlichen Pflichten untersucht. Auszüge aus den entsprechenden rechtlichen Regelungen finden sich in Anhang D.

6.1 Einleitung

Um das Potential von P2P-Netzen und -Systemen korrekt einzuordnen, stellt sich die Frage, welche Rechte und Pflichten für den Betrieb gelten. Rechtliche Untersuchungen im P2P-Bereich fokussierten bisher allerdings fast ausschließlich urheberrechtliche Gesichtspunkte. Ausführungen hierzu finden sich unter anderem in [Hoeren 2002] und [Wenzl 2005]. Wie in den Abschnitten 2.4 und 4.1 aufgezeigt wurde, umfasst das Einsatzspektrum von P2P-Systemen jedoch deutlich

mehr als Dateitauschsysteme (in diesem Sinne auch [Hoeren 2008, S. 156]).

Beim Betrieb von P2P-Systemen sind ebenso wie beim Betrieb von Rechnernetzen oder verteilten Informationssystemen bereichsspezifische rechtliche Regelungen zu berücksichtigen. Es existieren zahlreiche telekommunikationsrechtliche Regelungen, die unter anderem das Fernmeldegeheimnis, Verordnungen zur Telekommunikationsüberwachung oder telemedienrechtliche Informationspflichten[1] umfassen. Da durch P2P-Systeme die Grenze zwischen Netzwerken und Anwendungen zusehends verschwimmt [Peterson & Davie 2003, S. 680], besteht eine wesentliche Herausforderung darin, die einschlägigen Rechtsnormen[2], kurz Normen, zu ermitteln.

Dabei ist es nicht zielführend bzw. effizient, die rechtliche Diskussion unabhängig und nachgelagert zur Entwicklung des technischen Systems zu führen:

- Um den rechtlichen Anforderungen gerecht zu werden, kann unter Umständen eine Modifikation von Systemen oder des Betriebskonzepts notwendig werden. Finden solche Faktoren im Vorfeld Berücksichtigung, können teilweise langwierige Anpassungen vermieden werden.
- Existierende rechtliche Einordnungsschemata[3] und gesetzliche Regelungen orientieren sich an bestehenden Systemen und müssen daher im Rahmen der technischen Weiterentwicklung angepasst werden. Insofern ist die Berücksichtigung aktueller Technologien wie P2P-Techniken geboten. Andererseits sollte jedoch die notwendige Neutralität hinsichtlich einzelner Technologien gewahrt bleiben.

Letztlich ist es somit das Ziel der folgenden interdisziplinären Betrachtungen, die Entwicklung rechtskonformer Systeme zu erleichtern und durch adäquate Einordnung der technischen Sachverhalte die Grundlage für die (Fort-)Entwicklung angemessener Richtlinien und Gesetze zu eröffnen.

6.2 Hintergrund

In diesem Abschnitt werden die für die folgende technisch-rechtliche Analyse notwendigen Grundlagen wie der rechtliche Rahmen, Grundzüge der juristischen Methodik der Auslegung sowie eine funktionale Klassifikation von P2P-Systemen dargelegt.

[1] umgangssprachlich Impressumspflicht genannt

[2] Der Begriff Rechtsnorm wird zur Abstraktion genutzt und umfasst unter anderem Gesetze, Verordnungen und Richtlinien.

[3] auch als Interpretationen bezeichnet

6.2.1 Rechtlicher Rahmen

Im Gegensatz zu den bekannten Basisnetzen bilden P2P-Netze neue logische Netze oberhalb bestehender physischer oder logischer Netze und stellen somit die Grundlagen für neuartige Dienste der Informationsgesellschaft bereit. Insofern können P2P-Netze auch als Teilfunktionalität von so genannten Next-Generation-Networks (NGN)[4] betrachtet werden. Die Konvergenz von klassischem Telefonnetz (engl. Public Switched Telephone Network, PSTN) und Datennetzen führt zu NGN. Damit lassen sich sodann beliebige Dienste auf nur einem gemeinsamen Netz realisieren. Das Internet ist zwar auch ein paketvermittelndes Netz, jedoch können im Allgemeinen keine Garantien bezüglich der geforderten Bandbreite und Laufzeit gegeben werden, wie sie erforderlich wären. Ebenso kann eine sinnvolle Mobilitätsunterstützung oder nomadische Nutzung im heutigen Internet nur durch Zusatzdienste wie Mobile-IP, Verzeichnisdienste oder P2P-Netze erreicht werden, wohingegen gemäß der ITU-Definition [ITU NGN, Study Group 13] dies gerade eine entscheidende Rolle einnimmt, da nur so eine stetige und allgegenwärtige Dienstbereitstellung möglich ist.

Der Einbezug des allgemeineren Kontextes von NGN in die folgende Betrachtung bietet sich an, da zu anderen Themenbereichen wie VoIP schon verschiedene rechtliche Untersuchungen (vgl. [BNetzA 2005]) vorhanden sind, die zu Vergleichszwecken herangezogen werden können. Ferner erfordert die Gestaltung eines Einordnungsschemas die Berücksichtigung des Kontextes, um zu einer die Chancen und Risiken neuartiger Technologien ausgleichenden rechtlichen Lösung zu gelangen.

Die Kommunikation stellt eine zentrale Komponente der heutigen Informationsgesellschaft dar, die auch einen starken Wirtschaftsbezug aufweist. Daher handelt es sich um eine binnenmarktrelevante Sachmaterie, welche auf europäische Harmonisierung angelegt ist.

Die Europäische Union hat hinsichtlich elektronischer Kommunikationsnetze und -dienste deshalb ein Paket von Richtlinien [WWW eComm] erlassen, das aus einer so genannten Rahmenrichtlinie (RRL) und vier weiteren Richtlinien besteht:

- **Rahmenrichtlinie 2002/21/EG:** über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste [EU 2002/21/EG]

[4] Gemäß der ITU-Definition [ITU NGN, Study Group 13] basieren NGN auf einem paketvermittelnden Netz, das möglichst breitbandig sein sollte und bestimmte Dienstgüte-Parameter unterstützt. Dienstbezogene Funktionen sollten dabei unabhängig von dem unterliegenden Netz sein und Nutzern einen uneingeschränkten Zugang zu unterschiedlichen Diensteanbietern ermöglichen. Ferner sollte die Mobilität unterstützt werden, so dass ein ubiquitärer und konsistenten Dienstzugang möglich ist.

- **Zugangsrichtlinie 2002/19/EG:** über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung [EU 2002/19/EG]
- **Genehmigungsrichtlinie 2002/20/EG:** über die Genehmigung elektronischer Kommunikationsnetze und -dienste [EU 2002/20/EG]
- **Universaldienstrichtlinie 2002/22/EG:** über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten [EU 2002/22/EG]
- **Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EC:** über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation [EU 2002/58/EG]

Außerdem sind noch verschiedene Richtlinien hinsichtlich bestimmter rechtlicher Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt zu beachten. Zu diesen zählt insbesondere die **Richtlinie (98/34/EG)** [EU 98/34/EG] und die **e-commerce Richtlinie (2000/31/EG)** [EU 2000/31/EG].

Dabei ist jedoch zu beachten, dass Richtlinien ihre Wirkung nicht direkt gegenüber Bürgern und Unternehmen entfalten, sondern durch die Mitgliedsstaaten in nationales Recht umgesetzt werden müssen. Insofern hat die Beurteilung der rechtlichen Einordnung am nationalen Umsetzungsakt zu erfolgen. Allerdings sind die maßgeblichen Richtlinientexte sodann bei der Auslegung der gesetzlichen Vorschriften zu berücksichtigen. Für die Untersuchung in dieser Arbeit wurden deshalb primär die nationalen (deutschen) Normen zugrunde gelegt.

Die Umsetzung der Europäischen Richtlinien in der Bundesrepublik Deutschland erfolgt im Kern durch das **Telekommunikationsgesetz (TKG)** [TKG 2004] und das **Telemediengesetz (TMG)** [TMG 2007]. Nach der durch das Richtlinienpaket bedingten Novelle des TKG ist jetzt auch jüngst eine Anpassung der telemedienrechtlichen Vorschriften erfolgt [BT-Drs. 16/3635]. Bevor das TMG im März 2007 in Kraft getreten ist, wurde diese Rolle durch das *Teledienstgesetz (TDG)* [TDG 97] in Verbindung mit dem *Mediendienstestaatsvertrag (MDStV)* [MDStV 97] wahrgenommen, da bedingt durch die föderale Struktur die Bundesländer insbesondere für die Gesetzgebung in den Bereichen Rundfunk und Presse zuständig sind.

Wie im Abschnitt 6.3 noch näher ausgeführt wird, besteht infolge der unterschiedlichen rechtlichen Folgen die maßgebliche Herausforderung darin, eine Unterscheidung von so genannten **Telekommunikationsdiensten** (engl. Electronic Communication Service) und **Diensten der Informationsgesellschaft** (engl. Information Society Services) vorzunehmen. Der Unterschied besteht im Wesent-

lichen darin, dass beim Telekommunikationsdienst die Übertragung (der Signale) im Vordergrund steht, während beim Dienst der Informationsgesellschaft den übertragenen Inhalten eine entscheidende Rolle zukommt.

Im Zusammenhang mit Next-Generation-Networks (NGN) gewinnt zudem die Frage nach der "Netzneutralität" (vgl. u.a. [WWW save]) an erheblicher Bedeutung [Spies 2006]. Nach den derzeitigen Entwicklungen in den USA wird dieser Aspekt auch von der Europäischen Kommission im Rahmen der regelmäßigen Überprüfung des EU-Rechtsrahmens für elektronische Kommunikationsnetze und -dienste nach Art. 25 der Rahmenrichtlinie berücksichtigt [EU 2006a]. In der US-amerikanischen Diskussion wird im Schwerpunkt jedoch nur auf Aspekte des ungehinderten Informationszuganges abgestellt. Die Diskussion betrifft damit weitestgehend den regulatorischen Kontext herkömmlicher Telekommunikationsdienstleister im Verhältnis zu Inhalteanbietern im Internet und die möglichen Gefahren einer innovationshemmenden Diskriminierung neuer Dienste der Informationsgesellschaft.

Den im Rahmen der Diskussion zur Netzneutralität bezeichneten Diskriminierungsmitteln wie Port Blocking, Qualitätsverminderung und Bandbreitenbeschränkung (vgl. [Spies 2006]) sehen sich nun auch die Betreiber von Diensten in NGN ausgesetzt. Die diesbezügliche europäische Diskussion verengt sich bislang noch auf Fragen im Zusammenhang mit VoIP. So zeigt das Beispiel der AGB zu einem E-Plus Datentarif [Eplus Agb], dass die Nutzung von Datenverbindungen für VoIP unzulässig sein soll. Dieses Beispiel zeigt hinreichend deutlich das Diskriminierungspotential, welches Betreibern klassischer Kommunikationsinfrastrukturen im Verhältnis zu Anbietern funktional gleichgerichteter neuerer Dienste verfügbar ist. In der VoIP-Debatte wird nunmehr vielfach nicht beachtet, dass die dort aufgeworfenen Fragen nach dem einschlägigen Regulierungsregime dieser Dienste grundsätzlicher Natur für eine Vielzahl von Diensten in NGN sind und die Antworten mithin eine Weichenstellung für das Entwicklungspotential dieser neuen Dienstformen präjudizieren. So wird dann bislang in der öffentlichen Auseinandersetzung überwiegend vorgetragen, dass die nationalen Regulierungsbehörden mit der Ermächtigung des Art. 5 Abs. 1 der Zugangsrichtlinie Mittel an die Hand gegeben würden, derartige Diskriminierungen zu unterbinden. Dabei wird in der diesbezüglichen Stellungnahme der Bundesregierung im Rahmen der europäischen Evaluierung des EU-Rechtsrahmens für elektronische Kommunikationsnetze und -dienste bislang lediglich die Problemstellung als konkretisierungsbedürftig angesehen (vgl. [EU 2006a, S. 26] in Verbindung mit [EU 2006b]), was im Hinblick auf den raschen technologischen Fortschritt in diesem Bereich und das mögliche Innovationspotential dieser Dienste als unzureichend angesehen werden muss. Insofern kommt es für das konkrete Hand-

lungsinstrumentarium maßgeblich auf die Qualifikation der fraglichen Dienste an. Entweder sind sie als Telekommunikationsdienste, für welche der telekommunikationsrechtliche Rahmen der Zugangsregulierung unmittelbar einschlägig wäre, zu qualifizieren oder sie stellen sich im europäischen Rahmen als Dienste der Informationsgesellschaft dar, die diesem Regulierungsrahmen grundsätzlich nicht unterfallen. Für die regulatorische Verortung der Dienste kommen somit sowohl das Telekommunikations- als auch das Telemedienrecht in Betracht.

6.2.2 Rechtliche Auslegungsmittel

Da sich die gesetzliche Verortung an den Begriffen "Telekommunikationsdienst" gemäß TKG vs. "Telemediendienst" gemäß TMG festmacht, muss die jeweilige Reichweite der Begriffe ermittelt werden. Deshalb werden an dieser Stelle die wesentlichen Grundsätze einer rechtlichen Analyse, genauer Auslegung oder Interpretation, kurz dargelegt. Bei einer rechtlichen Auslegung werden im Allgemeinen vier klassische Formen der Auslegung unterschieden:

- *Grammatische Auslegung:* Ausgangspunkt einer jeden rechtlichen Auslegung ist der Wortlaut. Dabei ist fraglich, ob der gewählte Begriff eine Interpretation unter Zugrundelegung allgemein anerkannter grammatikalischer und semantischer Kriterien erlaubt.
- *Historische Auslegung:* Bei der historischen Auslegung wird vor allem die Fortentwicklung des Rechts anhand bisheriger Normen zugrunde gelegt.
- *Systematische Auslegung:* Ausgehend von dem Grundsatz, dass Normen widerspruchsfrei zueinander sein sollten, wird bei der systematischen Auslegung der Bezug zu anderen Normen untersucht.
- *Teleologische Auslegung:* Bei der teleologischen Auslegung wird letztlich untersucht, welcher Sinn und Zweck durch die Norm verfolgt.

Bei all diesen Arten der Auslegung muss insbesondere auch die existierende Literatur einschließlich der entwickelten Einordnungsschemata einbezogen werden.

6.2.3 Funktionale Klassifizierung von P2P-Systemen

P2P-Systeme lassen sich, wie in Abschnitt 2.3.2 dargestellt, in die beiden Schichten P2P-Netzwerke und P2P-Anwendungen aufteilen. Dabei versteht man unter P2P-Netzwerken selbstorganisierende Overlay-Netzwerke. Auf Basis dieser "universellen" P2P-Netze werden dann spezifische Funktionen durch die so genannten P2P-Anwendungen realisiert. Da P2P-Netze an sich universell einsetzbar sind, kann eine funktionale Klassifizierung nicht anhand des eingesetzten

P2P-Netzes erfolgen, sondern muss vielmehr das P2P-System als Ganzes berücksichtigen. Funktional können P2P-Systeme vor dem Hintergrund der hier fraglichen Dienstverortung in vier Bereiche unterteilt werden: i) die Lokalisierung von Nutzern bzw. Endsystemen und Vermittlung von Verbindungen, ii) die Lokalisierung von Inhalten bzw. Informationsdiensten, iii) die Weiterleitung von Datenpaketen und iv) die Bereitstellung von Inhalten.

Lokalisierung von Nutzern bzw. Endsystemen und Vermittlung von Verbindungen: Das Erfordernis der Lokalisierung von Nutzern bzw. Endsystemen ist dem Umstand geschuldet, dass Teilnehmer nicht mehr ausschließlich stationär arbeiten, sondern Netze und insbesondere das Internet zunehmend nomadisch nutzen. Zudem führen Techniken wie dynamische Vergabe von IP-Adressen und NAT-Router dazu, dass Internet-Nutzer nicht unter einer gleichbleibenden IP-Adresse erreichbar sind (vgl. Abschnitt 2.1). Vielmehr wird ein zweites Namens- bzw. Adressierungsschema genutzt, welches die Erreichbarkeit garantiert. Eine Kernfunktionalität solcher Dienste besteht somit in der indirekten Vermittlung von Verbindungen. Dabei wird die permanente Adresse eines zweiten Namensschemas mit Hilfe eines Verzeichnisservers auf eine dynamisch vergebene IP-Adresse abgebildet. Die permanente Adresse kann einem beliebigen Adressierungsschema entstammen, sie kann zum Beispiel aus dem Skype-Loginnamen gebildet werden. Diese P2P-Funktionalität ist vergleichbar mit der Funktionalität eines zentralistischen SIP-Servers[5] mit dem Unterschied, dass das Verzeichnis effizient auf die P2P-Knoten verteilt ist.

Lokalisierung von Inhalten bzw. Informationsdiensten: Ziel der zweiten Kategorie von P2P-Systemen ist es, Inhalte bzw. Informationsdienste zu lokalisieren. Die zweite Funktionalität unterscheidet sich von der Erstgenannten dadurch, dass die ermittelte Adresse angibt, auf welchem Zielsystem der gesuchte Inhalt bzw. Informationsdienst zu finden ist. Es wird also funktional eine "verteilte Suchmaschine" realisiert. Unter Informationsdiensten werden hierbei Dienste verstanden, welche bestimmte Inhalte zurückliefern bzw. Operationen auf bestimmten Inhalten ausführen. Solche Lokalisierungsfunktionalitäten werden bspw. in Gnutella (vgl. Abschnitt 2.4.2) oder von verteilten Dienstverzeichnissen angeboten (vgl. Abschnitt 4.1.2).

Weiterleitung von Datenpaketen: Weiterhin können P2P-Systeme auch zur direkten Weiterleitung von Datenpaketen genutzt werden. So werden bspw. im Fal-

[5] Hierbei ist insbesondere zu bemerken, dass in [RFC 3263] von "Locating SIP Servers" gesprochen wird.

le von Skype Datenpakete über ein drittes Peer ausgetauscht, wenn keine direkte Verbindung zwischen den Kommunikationspartner etabliert werden kann (vgl. Abschnitt 2.4.4). Auch die Internet Indirection Infrastructure (i3) beinhaltet diese Funktionalität [Stoica et al. 2002]. Im Gegensatz zu den beiden vorgenannten Kategorien, die nur beim Verbindungsaufbau eingesetzt werden, findet hier die gesamte Kommunikation über dritte Knoten des P2P-Systems statt.

Bereitstellung von Inhalten: Schlussendlich können P2P-Knoten Inhalte auch direkt bereitstellen und zwischenspeichern. Diese Funktionalität entspricht einem "verteilten Proxy". Das P2P-basierte System CoralCDN [WWW Coral] realisiert einen solchen verteilten Web-Proxy. Aber auch die klassische BitTorrent-Funktion zur Verteilung von Inhalten fällt unter diese Kategorie, da Inhalte bereitgestellt und zwischengespeichert werden.

6.3 Dienstverortung

Es stellt sich hinsichtlich der beschriebenen Funktionalitäten von P2P-Systemen die Kernfrage, ob jeweils Regelungen des Telekommunikationsrechts grundsätzlich als einschlägig zu erachten sind. Nahe liegend wäre es, im Hinblick auf die Ergebnisse der Diskussion um die Einordnung von Anwendungen des "klassischen" Internet wie zum Beispiel das World Wide Web (WWW) eine exklusive oder teilweise Zuordnung zum Telemedienrecht vorzunehmen (vgl. u.a. [Raabe 2003]).

Gegenstand der vorliegenden Untersuchung ist deshalb zunächst die Bestimmung der Reichweite des für die Anwendbarkeit des telekommunikationsrechtlichen Regelungsregimes maßgeblichen Begriffs des *Telekommunikationsdienstes* in § 3 Nr. 24 TKG. Dieser setzt den Begriff *elektronischer Kommunikationsdienst* aus Art. 2 lit. c) RRL in nationales Recht um. Da vielfach insbesondere zu VoIP-Diensten vertreten wird, dass Dienste, welche auf Anwendungsebene erbracht werden, grundsätzlich keine Telekommunikationsdienste seien, bedarf dieser Gesichtspunkt einer vertieften Betrachtung.

> "*Telekommunikationsdienste* [sind] in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen."
> gemäß § 3 Nr. 24 TKG

> "*elektronische Kommunikationsdienste* [sind] gewöhnlich gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze beste-

> hen, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen, jedoch ausgenommen Dienste, die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben; nicht dazu gehören die Dienste der Informationsgesellschaft im Sinne von Artikel 1 der Richtlinie 98/34/EG, die nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen"
> gemäß Art. 2 lit. c) RRL

Der ursprüngliche Ausgangspunkt der Schwierigkeiten bei der Verortung solcher Dienste entstand durch die Bestimmung des § 2 Abs. 4 Nr. 1 Teledienstgesetz (TDG)[6]. Dieser bestimmte nach seinem Wortlaut, dass die Regelungen des TDG nicht für Telekommunikationsdienste galten. Das hatte zur Folge, dass bei ausschließlicher Zugrundelegung des Wortlautes Dienste, die eine Doppelfunktionalität aufweisen, nicht vom Telekommunikationsgesetz erfasst werden [Raabe 2003]. Insofern sind in der Literatur verschiedene Abgrenzungskriterien entwickelt worden, um den jeweiligen Regelungsregimen einen randscharfen Anwendungsbereich zu eröffnen. Die Motivation hierfür ist jedoch entfallen, da der bundesrepublikanische Gesetzgeber in § 1 Abs. 1 TMG den Anwendungsbereich des TMG auch für solche Informations- und Kommunikationsdienste eröffnet hat, die nicht ausschließlich Telekommunikationsdienste nach § 3 Nr. 24 TKG sind. Damit kommt der Gesetzgeber einer Forderung aus der Literatur nach, eine Klarstellung auf die gegebenenfalls parallele Anwendung der beiden Regelungsbereiche herbeizuführen [Koenig & Neumann 2004, S. 3, 5 f].

Gleichwohl ist damit für die Frage, ob Dienste, die durch P2P-Systeme realisiert werden, dem Telekommunikationsrecht zuzuordnen sind, noch nicht viel gewonnen. Allerdings könnten die Kriterien, die in der Diskussion um die Abgrenzung der Regulierungsregime von TDG und TKG genannt wurden, für die Frage nach der Eingrenzung des Begriffs des Telekommunikationsdienstes gangbar gemacht werden.

Hinsichtlich der vorgenannten Funktionalitäten von P2P-Systemen soll dabei vor allem die Vermittlungsfunktionalität, welche durch P2P-basierte Verzeichnisdienste erbracht wird, im Mittelpunkt stehen. Diese Dienste können auf menschliche Wahrnehmung ausgelegt sein, was auf einen Informationsdienst im Sinne des TMG hinweist, und stellen gleichzeitig mittels der Zuweisung von Adressdaten eine technische Vermittlungsinstanz dar, was auf eine Zuordnung zum TKG schließen lassen könnte. Damit gehören solche Dienste bei oberflächlicher Sicht eindeutig in den Kreis der fraglichen Dienstfunktionalitäten.

[6] Das Teledienstgesetz wurde mittlerweile durch das Telemediengesetz (TMG) abgelöst.

Entsprechend der Legaldefinition[7] des § 3 Nr. 24 TKG sind "Telekommunikationsdienste in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen". Durch dieser Formulierung enthält die Definition einen technischen und einen wirtschaftlichen Gesichtspunkt, die jeweils anhand der vorgenannten juristischen Auslegungsmittel interpretiert werden müssen. Bevor insofern ein eigener Lösungsansatz dargelegt wird, werden die Dienstfunktionalitäten zunächst an den herkömmlichen Eingrenzungsmaßstäben gemessen.

6.3.1 Lösung nach klassischen Kriterien

Zuordnung nach fachwissenschaftlichen Kriterien

Bei der Bestimmung, welche Dienste der "Übertragung von Signalen" dienen, ist es hinsichtlich des vorgenannten Wortlautarguments nahe liegend auf den Sprachgebrauch der einschlägigen Fachwissenschaften abzustellen. Aus dem Wortlaut der Legaldefinition des Begriffs der "Telekommunikation" in § 3 Nr. 16 TKG alte Fassung (a.F.) [TKG aF] und in Zusammenschau mit der Legaldefinition des § 3 Nr. 17 TGK a.F. wurde auf Grundlage des physikalischen Signalbegriffs eine konkretisierte Legaldefinition der Telekommunikation entwickelt. Hiernach ist ein Telekommunikationsdienst das Angebot der Signalübertragung zwischen zwei physisch definierten Punkten mittels technischer Einrichtungen und Systemen. Im Umkehrschluss wird gefolgert, dass ein Dienst, der keine eigenständige unmittelbare Raumüberwindung anbietet, kein Telekommunikationsdienst sei [Koenig & Neumann 2004, S. 7]. Da das novellierte TKG [TKG 2004] insofern keine Veränderung erfahren hat [Heun 2003, S. 487], sollte diese konkretisierte Legaldefinition auch für das geltende Recht anwendbar sein [Koenig & Neumann 2004, S. 25].

Legt man diese Betrachtungsweise zugrunde, würden P2P-Systeme, welche die Vermittlung von Verbindungen und das Bereitstellen und Zwischenspeichern von Inhalten zum Gegenstand haben, schon nach dem Wortlaut nicht oder nicht ausschließlich als Telekommunikationsdienste einzuordnen sein. Das Angebot von SIP-Verzeichnisservern und Skype wäre bspw. nicht als Telekommunikationsdienst anzusehen. Da die Verwendung eines Verzeichnisservers selbst keinen unmittelbaren Beitrag zur Raumüberwindung beim Kommunikationsakt leistet, wäre eine Zuordnung hiernach nicht möglich. Im Gegensatz hierzu sieht die Bundesnetzagentur in VoIP nur eine andere Technik, so dass es sich aufgrund der Technikneutralität folglich um Telekommunikation handelt [BNetzA 2005, S. 5].

[7] Wenn in einem Gesetz selbst die Definition eines Rechtsbegriffes vorgenommen wird, nennt man dies Legaldefinition.

Nach der vorgenannten Definition wären P2P-Systeme allenfalls dann als Telekommunikationsdienste zu klassifizieren, wenn sie selbst Datenpakete weiterleiten (in diesem Sinne vermutlich [Holznagel & Bonnekoh 2005, S. 590]), wie das im Rahmen der Internet Indirection Infrastructure der Fall ist.

Zuordnung nach dem ISO/OSI-Schichtenmodell

Eine andere in der Literatur entwickelte Auslegung orientiert sich in Hinblick auf den vermuteten Zweck der Regelungen an der Zuordnung der Dienste im ISO/OSI-Schichtenreferenzmodell [Zimmermann 1980; ISO/IEC 7498-1]. Hiernach sind Funktionalitäten, die oberhalb der Schicht 4 des Referenzmodells erbracht werden, nicht mehr dem Begriff der Telekommunikation zuzuordnen, sondern als Telemediendienste anzusehen. Damit wären sie aber im Ergebnis, wegen der Realisierung von P2P-Systemen auf Anwendungsebene (Schicht 7), in keinem Fall als Telekommunikationsdienste anzusehen (vgl. hierzu [Helmke et al. 1998], [Raabe 2003]; ablehnend hingegen [Möller 2000]).

Zuordnung nach ökonomischen Kriterien

Daneben werden die genannten Dienste teilweise auch pauschal anhand des zweiten Bestandteils der Legaldefinition, der Frage nach der Entgeltlichkeit des Dienstes, ausgeschieden. Es wird also schon auf der Ebene der Legaldefinition ausschließlich auf das Geschäftsmodell der P2P-Betreiber abgestellt. Danach scheiden im Ergebnis solche Dienste aus, bei denen keine Kommunikation in das PSTN angeboten wird. Da die diesbezüglichen Untersuchungen auf VoIP basieren, wird die Entgeltlichkeit hierbei am Angebot eines Übergangs zum PSTN festgemacht. Es wird beim Fehlen dieses Übergangs entweder die Betreibereigenschaft verneint [Holznagel & Bonnekoh 2005, S. 590] oder das Vorliegen eines Telekommunikationsdienstes bei der Bereitstellung von kostenlosen Softwareapplikationen am Merkmal "in der Regel nicht gegen Entgelt" ausgeschieden. Kostenfrei angebotene Dienste fallen somit aus dem telekommunikationsrechtlichen Rahmen [Meinberg & Grabe 2004, S. 413].

Der österreichische Regulierer, die RTR-GmbH [WWW RTR], stellt insofern den Dienstcharakter eines VoIP-Angebots mit dem Argument in Abrede, dass, wenn im Wesentlichen nur die IP-Adresse des gerufenen Teilnehmers verfügbar gemacht werde, der angebotene Dienst nicht ganz oder überwiegend in der Übertragung von Signalen bestehe, soweit kein entsprechendes Kostenelement für die Übertragung im VoIP-Dienst enthalten sei [RTR 2006, S. 63ff]. Das Gewicht dieses Argumentes lässt sich allerdings nur mit der divergierenden Umsetzung des Art. 2 lit. c) RRL erklären. Während die Richtlinie noch von "ge-

wöhnlich gegen Entgelt" erbrachten Diensten spricht, was im Ergebnis auch der Wertung der deutschen Regelung des § 3 Nr. 24 TKG entspricht, hat der österreichische Gesetzgeber mit dem Abstellen auf "gewerbliche Dienstleistungen" in § 3 Nr. 9 des österreichischen Telekommunikationsgesetzes [TKG-Oe] eine deutlich weitergehende Einengung des Begriffs des Telekommunikationsdienstes auf der ökonomischen Ebene erreicht, welche nicht der Intention des Richtliniengebers entsprechen dürfte.

Nach allgemeinen Auslegungsgrundsätzen ist davon auszugehen, dass der Ausnahmetatbestand "in der Regel" eine enge Auslegung fordert. Ob die Konsequenz des Ausscheidens der Vermittlungsdienste aus dem regulatorischen Kontext des Telekommunikationsrechts bei lediglich mittelbaren Gewinnerzielungsabsichten vom Gesetzgeber gewollt ist, erscheint aus historischer und systematischer Sicht jedoch fraglich. In der Begründung zur Änderung des TKG wurde insofern mit der Einfügung eines § 110 Abs. 1 Nr. 1a TKG der Umstand anerkannt, das bspw. bei der VoIP-Telefonie die zur Steuerung einer Telekommunikation erforderlichen Signale und die Signale, die den Nachrichteninhalt repräsentieren, über völlig voneinander getrennte Telekommunikationsanlagen übermittelt werden können [BR-Drs. 359/06]. Damit scheint der Gesetzgeber über den Anschluss ans Datennetz hinaus auch einen exekutiven Zugriff auf reine SIP-Server ermöglichen zu wollen. Dies wäre bei einem Ausscheiden der Betreiber der Verzeichnis- bzw. Lokalisierungsserver auf der Ebene des § 110 TKG nicht möglich.

Insofern ist mit einer weiteren Stimme aus der Literatur davon auszugehen, dass jedenfalls die alternative Erzielung von wirtschaftlichen Vorteilen kein Ausschlusskriterium für die Klassifizierung als (Tele-) Kommunikationsdienst sein kann [Seitlinger & Strobl 2005]. Für eine enge Interpretation im Rahmen der Legaldefinition besteht aus systematischen Gründen auch kein Bedürfnis, weil durch Formulierungen wie "Telekommunikationsdienste für die Öffentlichkeit" im Rahmen der Tatbestände der §§ 47, 110 TKG bzw. der "gewerblichen Telekommunikationsdienste für die Öffentlichkeit" § 6 Abs. 1 TKG eine diesbezüglich sinnvolle Eingrenzung auf Ebene der materiellen Regelungen erfolgt. Schließlich ist das Abstellen auf die Verbindung zum PSTN auch deshalb nicht zielführend, da sich das klassische PSTN zunehmend auflöst und in NGN aufgeht.

Zwischenergebnis

Zusammenfassend ist also davon auszugehen, dass das ökonomische Merkmal der Legaldefinition, jedenfalls bei alternativer Erzielung von wirtschaftlichen Vorteilen durch den Betrieb von P2P-Applikationen, als gegeben angesehen werden kann. Zudem hat sich gezeigt, dass nach herkömmlicher Betrachtung des technischen Bestandteiles der Legaldefinition Dienste in P2P-Netzwerken dem tele-

kommunikationsrechtlichen Regulierungsrahmen weitestgehend nicht unterliegen. Wegen der funktionalen Gleichrichtung mit klassischen Telekommunikationsdiensten erscheint dieses Ergebnis jedoch als nicht tragfähig. Es soll deshalb im Folgenden untersucht werden, inwiefern sich ein sachgerechter Lösungsansatz entwickeln lässt .

6.3.2 Lösung nach dem Ende-zu-Ende-Paradigma

Ausgangspunkt einer alternativen Betrachtung ist die Feststellung, dass in IP-Netzen die Intelligenz zunehmend vom Zentrum in die Peripherie wandert (vgl. bspw. [Kurose & Ross 2004, S. 125] und [Kurth 2003]). Diesem Umstand muss bei der Auslegung von Normierungen des Telekommunikationsrechts, die nach wie vor durch den Blick auf das PSTN geprägt sind, Rechnung getragen werden.

Der Paradigmenwechsel zeigt sich schon beim Domain Name System (DNS). Die DNS-Server sind zwar auf der Anwendungsschicht realisiert, gelten aber dennoch aus technischer Sicht heute als ein integraler Bestandteil des Internet[8]. Hierbei wird ein grundlegendes Entwurfsmuster des Internet deutlich, das so genannte *End-to-End Argument*. Saltzer, Reed und Clark formulierten dieses Entwurfsmuster in ihrer Arbeit von 1984 [Saltzer et al. 1984]. Die Kernaussage dieser fundamentalen Arbeit ist: "Die fragliche Funktion kann nur komplett und korrekt implementiert werden mit dem Wissen und der Hilfe der Applikation, welche an den Endpunkten des Kommunikationssystems steht. Aus diesem Grund kann die fragliche Funktionalität nicht als Merkmal durch das Kommunikationssystem selbst erbracht werden." [Saltzer et al. 1984, S. 278]. Zusammenfassend soll also eine Funktionalität nur dann auf einer niedrigeren Schicht implementiert werden, wenn sie dort vollständig und korrekt implementiert werden kann [Peterson & Davie 2003, S. 381][9]. Das Ende-zu-Ende-Argument gilt aber nicht nur für "direkte" Verbindungen, wie bspw. TCP-Verbindungen zu einem Web-Server, sondern auch für Verbindungen über einen intermediären Server [Blumenthal & Clark 2001, S. 80 f]. Ein Beispiel hierfür stellt die E-Mail-Kommunikation dar. Die E-Mail-Kommunikation erfolgt über SMTP-Server, die auf der Anwendungsschicht implementiert sind. Dennoch stellen sie im Sinne des Ende-zu-Ende-Arguments nur Zwischensysteme dar und die Enden der Kommunikation sind das sendende und das empfangende System.

Insofern wird in [Blumenthal & Clark 2001] gefolgert, dass das Ende-zu-Ende-Paradigma mit den Basisprotokollen des klassischen Internet nicht mehr umsetzbar ist. P2P-Netze bzw. Systeme helfen diesem Problem ab, ohne tiefgreifende

[8] David Clark führt hierzu folgendes aus: "The DNS is not part of the specification of IP, but most would consider it to be a part of the Internet." in [Clark 2005]

[9] Siehe insofern auch die instruktive Analyse bei van Schewick in [v. Schewick 2005, S. 87ff].

Änderungen im Netz zu erfordern (vgl. u.a. [Peterson & Davie 2003, S. 680 ff] oder [Steinmetz & Wehrle 2005b, S. 10]). Hierbei ist insbesondere die Vermittlung von Verbindungen, d.h. die Abbildung von einem Namensschema auf IP-Adressen durch Verzeichnisserver essentiell.

Das Ende-zu-Ende-Paradigma und das ISO/OSI-Referenzmodell

Wird bei der Beurteilung von Dienstfunktionalitäten nach dem Ende-zu-Ende-Paradigma die klassische Einordnung im Sinne des Schichtenmodells zugrunde gelegt, würden sich diese P2P-basierten Dienste, wie gezeigt, der Verortung im Kontext des Telekommunikationsrechts entziehen.

Allerdings sind Ordnungsstrukturen, die in technischen Beschreibungsmodellen abgebildet werden, selbst in der Informatik nicht als starre normative Vorgaben aufzufassen. So enthält bspw. das klassische ISO/OSI-Schichtenmodell sieben Schichten[10]. Das verkürzte Internet Schichtenmodell beinhaltet hingegen nur vier Schichten (vgl. u.a. [Peterson & Davie 2003, S. 28] oder [Science & Board 1994, S. 47 ff]). Ergänzt man dieses Internet-Schichtenmodell mit verfügbaren oder möglichen Protokollen, so fällt auf, dass sich durch das IP-Protokoll eine Art Sanduhr bildet (vgl. [Deering 1998] bzw. [Science & Board 1994, S. 51 ff]). Auf Schicht 3 gibt es nur ein einziges Protokoll, nämlich das IP-Protokoll, während auf den darüber und darunter liegenden Schichten verschiedene Protokolle genutzt werden.

So weist nunmehr Clark darauf hin, dass man im Hinblick auf die technische Entwicklung nicht zwangsläufig am Schichtenmodell festhalten muss, sondern auch Alternativen zur Verfügung stehen. Das Schichtenmodell sei daher nur als Entwurfsmuster zu sehen, welches in Zukunft auch durch ein anderes ersetzt werden könne [Clark 2005]. Auch die Bundesnetzagentur geht nach der Auswertung der Ergebnisse der Anhörung zu VoIP nunmehr davon aus, dass eine telekommunikationsrechtliche Einordnung von VoIP-Diensten nicht allein auf Grundlage des ISO/OSI-Modells vorgenommen werden kann und es lediglich eine Orientierungshilfe darstellt [BNetzA 2006, Nr. 15]. Dies spricht schon dagegen, das ISO/OSI-Modell in der juristischen Diskussion als normativ zu begreifen.

Bei Anwendung des systematischen Argumentes wird dieses Ergebnis durch die Begründung des TMG-E gestützt, wonach Internet-Telefonie keinen Unterschied zur herkömmlichen leitungsgebundenen Telefonie aufweise und als reine TK-Dienstleistung anzusehen sei [TMG-E, S. 13]. Dies streitet für die Vermutung, dass bei funktional gleichgerichteten Aktivitäten auf Applikationsebene gleichwohl das Telekommunikationsrecht einschlägig sein kann. Insofern stellt sich die

[10] Die sieben Schichten des ISO/OSI-Referenzmodell entstanden letztlich auch als Kompromiss zwischen sechs und acht Schichten [Peterson & Davie 2003, S. 196].

Frage, ob für reine Vermittlungsaktivitäten durch P2P-Systeme auf Basis eines verteilten Verzeichnisses etwas anderes gelten darf. Wenn aber die Einordnung nach dem Schichtenmodell sich als nicht hinreichend tragfähig erweist, bedarf es für die Rechtsanwendung eines anderen Eingrenzungsmaßstabes.

Das Ende-zu-Ende-Paradigma und der Begriff Signalübertragung

Dienste wie SIP- oder Verzeichnisserver, die nur einen *mittelbaren* Einfluss auf das Routing der Datenpakete und mithin der Signalübertragung im eigentlichen Sinne nehmen, wären, wie oben ausgeführt, bei Zugrundelegung eines engen Begriffs der Signalübertragung auszuscheiden.

Aus historischer Perspektive stellt sich die Frage, ob insofern der Ansatz einer konkretisierten Legaldefinition, der im Ergebnis einen Telekommunikationsdienst ausschließlich bei einem *unmittelbaren* Beitrag zur Raumüberwindung annimmt, dem Willen des Richtliniengebers entspricht.

Die Verbindungssteuerung der Ende-zu-Ende-Kommunikation bezieht sich, jedenfalls aus technischer Sicht, nicht ausschließlich auf das IP-Routing der Datenpakete, sondern kann auch die Ermittlung der aktuell gültigen IP-Adresse der Beteiligten der Kommunikation erfordern. Die klassische "Steuerung des Leitweges" durch den Anbieter im PSTN wird hierbei durch die "Vermittlung" der aktuellen Adressierungselemente der Kommunikationsteilnehmer substituiert. Dieses Beispiel zeigt deutlich den Kern des Ende-zu-Ende Arguments. Diese "Vermittlungsfunktion" kann sinnvoller Weise nicht in das Basisnetz integriert werden.

Einbezug des Routing: Legt man diesen Maßstab an die Grunddefinition des Telekommunikationsdienstes an, dann ist ersichtlich, dass eine enge Auslegung des Begriffs der "Signalübertragung" diesem Umstand nicht hinreichend gerecht werden kann. Wenn man anerkennt, dass neben der Steuerung der Übertragungssysteme auf Schicht 1 und 2 des ISO/OSI-Modells auch das Routing der entsprechenden digitalen Signalen oberhalb dieser Schicht dem Begriff der Signalübertragung zuzurechnen sein soll, kann die zielgerichtete Weiterleitung der Datenpakete und die Generierung der notwendigen Routing-Informationen auseinander fallen. So findet bei der Internet-Kommunikation die Weiterleitung der Datenpakete (engl. Forwarding) mit Hilfe von so genannten Weiterleitungstabellen (engl. Forwarding Tables) statt, während die Generierung der darin enthaltenen Routing-Informationen durch Routing-Protokolle wie zum Beispiel OSPF oder BGP in parallelen Prozessen erfolgt [Aweya 2001]. Eine solche Beeinflussung des Routing der Datenpakete würde, da sie nicht vollständig auf dem routenden Rechner selbst stattfindet, bei einer engen Auslegung aus dem Übertragungsbegriff auszuscheiden sein.

Die der deutschen Regelung zugrunde liegende Rahmenrichtlinie, die im Rahmen des historischen Arguments zu berücksichtigen ist, zeigt ausdrücklich mit ihrem technologieneutralen Ansatz und der Integration des Internet in die Netzdefinition des Art. 2 lit. a) RRL, dass von ihr *auch* paketvermittelte Kommunikation mit Routing auf logischer Ebene erfasst sein soll. Insofern ist also davon auszugehen, dass der Prozess der mittelbaren Verbindungssteuerung durch Dienste, welche selbst nicht zwingend das Forwarding betreiben müssen, in die Dienstdefinition aufzunehmen ist.

Hiergegen streitet nicht, dass im ersten Entwurf der RRL [EU 2001/C 96/02] durch die Kommission noch die Leitweglenkung ("Routing") neben der Übertragung von Signalen als integraler Bestandteil der Dienstdefinition aufgeführt wurde. Später ist dieser Definitionsbestandteil sodann zwar ohne Begründung entfallen. Es ist jedoch nahe liegend, dass dies nicht zuförderst deshalb geschehen ist, um die Steuerung des Weges von Datenpaketen als notwendige Annextätigkeit aus dem Dienstbegriff auszuklammern. Vielmehr dürfte dies dem Umstand geschuldet sein, dass es auch Diensteanbieter geben kann, die selbst kein Kommunikationsnetz betreiben und deshalb selbst kein Routing der Datenpakete vornehmen.

Einbezug mittelbar steuernder Systeme: Es stellt sich vor diesem Hintergrund sodann die Folgefrage, ob bei dieser Form des Routings die nur *mittelbar* steuernden Systeme in den Dienstbegriff aufgenommen werden können, wie das bspw. bei einer rein adressauflösenden Tätigkeit wie dem DNS der Fall wäre.

Auch in Netzen der klassischen Telefonie kann die Steuerung der Signale und die eigentliche Raumüberwindung auseinander fallen. Dies zeigt sich leicht nachvollziehbar am Beispiel der GSM-Netze. Sie ermöglichen den Nutzern sowohl digitale Sprach- als auch Datendienste mobil zu nutzen. Eine grundlegende Funktion stellt dabei die Lokalisierung der Nutzer dar [Schiller 2000, S. 163].

Soll ein Anruf aus dem PSTN einem Teilnehmer im GSM-Netz zugestellt werden, wird dieser Anruf zunächst im PSTN bis zum Gateway Mobile Switching Center (GMSC) des zuständigen Mobilfunkanbieters zugestellt [Schiller 2000, S. 163 ff]. Die Auswahl des GMSC erfolgt anhand der Telefonnummer des Teilnehmers, die im Fall von GSM als MSISDN bezeichnet wird. Danach wird der Standort des Nutzers durch das so genannten Home Location Register (HLR) in Kombination mit dem Visitor Location Register (VLR) ermittelt. Diese Verzeichnisse beinhalten unter anderem nach der Registrierung durch den Nutzer somit immer den aktuellen Standort und eine zugehörige temporäre Nummer, die so genannte Mobile Station Roaming Number. Der eigentliche Datenaustausch findet hingegen nicht über das HLR statt, sondern die Verbindung wird dann di-

rekt über das GMSC aufgebaut. Insofern weist diese Lokalisierungsfunktionalität große Parallelen zur beschriebenen Vermittlungs- und Lokalisierungsfunktion durch P2P-Systeme auf.

Damit wird aber auch in diesem Fall der "klassischen" Telekommunikation der Begriff der "Signalübertragung" nicht mit "Durchleitung" übersetzt, sondern beinhaltet auch die *mittelbare Steuerung*. Diese Steuerung ist in paketvermittelnden Netzen wie dem Internet maßgeblich durch das gegebenenfalls auch entfernt gesteuerte Routing und die Zuweisung von Nummern wie zum Beispiel IP-Adressen für Netzabschlusspunkte bestimmt.

Systematische und teleologische Aspekte: Da damit im Rahmen des Ende-zu-Ende-Paradigmas die gegebenenfalls vom durchleitenden System separiert realisierte Adressauflösung die Definition des Telekommunikationsdienstes maßgeblich beeinflusst, erweist es sich aus systematischer Sicht auch als schlüssig. Neben dem Rufnummerbegriff des klassischen PSTN in § 3 Nr. 18 TKG erhält unter dieser Ägide auch der Nummernbegriff des § 3 Nr. 13 TKG einen sinnvollen Anwendungsbereich. Dabei steht nicht mehr in Frage, dass jedenfalls die IP-Adressen dem Nummernbegriff zuzuordnen sind[11]. Wie sich aus der Gesamtschau mit § 66 Abs. 1 Satz 3 TKG ergibt, kann aber jedwedes Adressierungsschema, grundsätzlich also auch Domainnamen[12], der Adressierung in Kommunikationsnetzen dienen, jedenfalls soweit diese auf höheren Schichten realisierten "virtuellen Netze" als Telekommunikationsnetze im Sinne von § 3 Nr. 27 TKG verstanden werden.

Die Freistellung der Toplevel-Domains (wie .de) sowie der nachgeordneten Domainnamen von der Regulierung steht dem nicht entgegen. Die Ausnahme stellt sich vielmehr als Systembruch dar, der eher gewachsenen Ordnungsstrukturen der Domainnamenvergabe durch die DENIC geschuldet ist, als dass er die grundsätzliche Zuordnung in Frage stellen könnte[13]. Eine positivrechtliche Einschränkung durch die gesetzliche Festlegung auf bestehende Adressierungsschemata kann aufgrund eines ausdrücklich entwicklungsoffen gestalteten Nummerierungsbegriffs [BT-Drs. 16/2581, S. 39] und vor dem Hintergrund des Ende-zu-Ende-Paradigmas nicht gewollt sein. Eine andere Frage ist, ob sodann tatsächlich eine materielle Regelung zur Regulierung greifen soll. Dies wird in der Kritik an der grundsätzlichen Einbeziehung von Domainnamen in den Nummerbegriff verkannt [eco Verband der deutschen Internetwirtschaft e.V. 2004, S. 9]. So übersteigt ausweislich der Gesetzesbegründung zur Änderung des TKG [BT-Drs. 16/2581, S. 22] der materielle Regelungsgehalt des § 66 TKG eben nicht den eu-

[11] Anderer Ansicht [Meinberg & Grabe 2004, S. 413]

[12] Anderer Ansicht [Koenig et al. 2003, S. 66]

[13] Anderer Ansicht, allerdings im Hinblick auf den Entwurf einer Telekommunikations-Nummerierungsverordnung (TKNV) [Heun 2003, S. 494]

roparechtlichen Rahmen[14]. Danach soll für den Bereich ENUM die Integrität des deutschen Rufnummernplanes im Rahmen der noch ausstehenden Zustimmung zum Wirkbetrieb gegenüber der ITU sichergestellt werden. Diese entspricht dem gesetzlich geforderten strukturierenden Element und ist durch Art. 10 Abs. 5 RRL ausdrücklich gedeckt. Ebenso wie eine Verwaltung von Domainnamen aufgrund ausdrücklicher Anordnung zulässig wäre, wird die zwingende Verwaltung von IP-Adressräumen oder anderen Adressierungsschemata im Internet in der Praxis nicht zu erwarten sein. Dies ergibt sich schon aus der praktischen Unmöglichkeit aufgrund bestehender, globaler, faktischer Normsetzung durch die ICANN (Internet Corporation for Assigned Names and Numbers) in diesem Bereich. Dies spricht aber nicht dagegen bspw. bei der Entwicklung neuartiger Adressierungsschemata in P2P- bzw. Overlay-Netzen unter der Prämisse eines knappen Namensraums grundsätzlich diese Möglichkeit auch der staatlichen Verwaltung zu eröffnen, wobei die Autoren in [Koenig & Neumann 1999, S. 148, 151] den Regulierungsbedarf bei IP-Adressen zu Recht bezweifeln.

Eine weite Auslegung der Dienstdefinition ist neben historischen und systematischen Argumenten auch aus teleologischen Gesichtspunkten angebracht. Die in § 1 TKG als Ziel beschriebene Technologieneutralität als bestimmendes Element des gesetzlichen Rahmens spricht dagegen, bei *funktional gleichgerichteten Tätigkeiten* schon auf der Ebene der Dienstdefinition bestimmte Anwendung aus dem regulatorischen Kontext auszuscheiden.

Overlay-Netze als Telekommunikationsnetze

Somit kommt es schlussendlich jedenfalls für die regulatorische Verortung von "Vermittlungsdiensten" in Overlay-Netzen auf die Konkretisierung des telekommunikationsrechtlichen Netzbegriffes an. Nach dem Wortlaut des § 3 Abs. 1 Nr. 27 TKG liegt es nahe, nur Basisnetze, wie das klassische PSTN, in der Grunddefinition zu verorten. Allerdings sollen nach der Gesetzesbegründung [BT-Drs. 15/2316, S. 58] und ausdrücklich nach dem Wortlaut des Art. 2 Abs. 2 a) RRL auch logische Netze wie das Internet dem Netzbegriff zuzuordnen sein.

Enge Auslegung: "Internet" als logisches IP-Netz: Mit der Erwähnung des Internet als logisches Netz über Basisnetzen wird der Anwendungsbereich für höhere logische Netze grundsätzlich eröffnet. Als erste Konsequenz leitet sich hieraus mit Blick auf das Ende-zu-Ende-Paradigma ab, dass der Abschlusspunkt dieser Netze nicht mehr an der physischen Schnittstelle des jeweiligen Rechners zu verorten ist. Vielmehr kann dieser Punkt auf dem Endsystem auch in einer höheren

[14] So aber [Koenig et al. 2003, S. 40] und [eco Verband der deutschen Internetwirtschaft e.V. 2004, S. 3]

Protokollschicht allein durch Software realisiert werden. Allerdings könnte vor dem Hintergrund einer engen Begriffsdefinition des Internet "als durch das IP-Protokoll definierten Signalübertragungsnetzes" lediglich eine Erweiterung des Netzbegriffes auf Schicht 3 des ISO/OSI-Modells erfolgen [Loetz & Neumann 2003, S. 7]. Insofern wird auch vertreten, dass weitere, auf dieser logischen Verbindung aufsetzende logische Verbindungen, die keine zusätzliche Raumrelevanz entfalten und daher keine neuen Netzabschlusspunkte bilden, aus dem telekommunikationsrechtlichen Rahmen auszuscheiden sind [Loetz & Neumann 2003, S. 7].

Weite Auslegung: "Internet" als virtuelles Netz: Die Einbeziehung weiterer, auf höheren Schichten realisierter, logischer Netze ist somit zwar nicht schon deshalb zwingend geboten, um der Bestimmung des Art. 2 a) RRL überhaupt einen sinnvollen Anwendungsbereich zu eröffnen. Allerdings verschließt die Normierung auch nicht den Weg, weitere logische Netze, die auf Anwendungsschicht realisiert werden, in ihren Anwendungsbereich aufzunehmen. So wird bei VPNs IP über IP genutzt, was eine Einbeziehung des VPN als logisches Netz nahelegt.

Auf welcher Ebene des Schichtenmodells ein logisches IP-Netz im Sinne der Definition realisiert wird, ist nunmehr nicht ausdrücklich bestimmt. Im Gegenteil wäre es wegen des technologieneutralen Ansatzes der RRL verfehlt, funktional gleichgerichtete Tätigkeiten, bei denen von den Inhalten gleichartig abstrahiert wird und der Signalcharakter der übertragenen Datenpakete identischer Natur ist, nur aufgrund der Realisierung in einer höheren Schicht des Schichtenmodells aus dem telekommunikationsrechtlichen Rahmen zu weisen.

Insofern zeigt aus systematischer Sicht der Wortlaut des Art. 2 a) der Zugangsrichtlinie den richtigen Weg. Dort wird mit dem Zugang zu "virtuellen Netzen" eine umfassendere Begrifflichkeit gewählt und intendiert, dass allgemein virtuelle Netze, ohne verengende Zuordnung zur technischen Realisierung des "Internet" heutiger Prägung bzw. der Paket- oder Leitungsvermittlung im klassischem Sinne, die Zielrichtung der Grunddefinition sind. Vielmehr sind auf Grundlage einer weiten Definition auch "virtuelle Verbindungen" (Virtual Circuits) denkbar, die wiederum als Basisnetz eine Paketvermittlung nutzen, wie es auch bei ATM[15] der Fall ist.

Erkennt man somit als Vorgabe an, dass wegen der funktionalen Gleichrichtung grundsätzlich auch Netze auf höherer Ebene als Schicht 3 des ISO/OSI-Modells dem Begriff des logischen Netzes zugeordnet werden können, kann es aber auf das verwendete Namensschema zur Adressierung bei Paketvermittlung

[15] ATM (Asynchronous Transfer Modus) ist eine paketvermittelte Technologie, die garantierte Dienstgüte ermöglicht und hauptsächlich im Backbone von klassischen PSTN-Netzen eingesetzt wird bzw. wurde (vgl. u.a. [Peterson & Davie 2003, S. 192 ff])

oder "virtueller Verbindungen" in dem höheren Netz nicht ankommen[16]. Ob hier erneut das IP-Schema oder eine Adressierung anhand von anderen, das Routing der die virtuellen Signale repräsentierenden Datenpakete beeinflussenden Namensschemata erfolgt, muss insofern unerheblich sein. Aus systematischer Sicht ist, wie bereits oben ausgeführt, insofern auch schlüssig, dass jedwedes Adressierungsschema in die Nummerndefinition des § 3 Nr. 13 TKG aufgenommen und bei knappen Ressourcen auch grundsätzlich einer hoheitlichen Verwaltung unterworfen sein kann. Ohne die verengte Sicht auf IP-Adressen oder Rufnummern wird dort anerkannt, dass auch sonstige Zeichenfolgen der Adressierung in Telekommunikationsnetzen dienen können. Eine Sicht die im Rahmen der Netzdefinition auf höherer Ebene allein Paketvermittlung unter dem Adressierungsschema IPv4 oder IPv6 anerkennt, würde somit aus systematischer Sicht nicht der gesetzlichen Wertung entsprechen.

Für die telekommunikationsrechtliche Würdigung der hier interessierenden Vermittlungsdienste ist vor diesem Hintergrund weiterhin von Gewicht, dass zu einem Netz nicht nur Übertragungswege gehören, sondern auch die Endpunkte. Diese Endpunkte werden ihrerseits durch Nummern bzw. Adressen definiert. Die Nummerierung ist dabei unabdingbare Voraussetzung für den Betrieb eines [zusammenhängenden] Netzes [VG Köln 2002, S. 371], wobei die Netzabschlusspunkte, nach dem vorher gesagten, ganz allgemein durch den Namen bzw. die Nummer im jeweils relevanten Protokoll bezeichnet werden.

Für Overlay-Netze bedeutete dies, dass sie grundsätzlich der Netzdefinition des § 3 Nr. 27 TKG zuzuordnen sind. Um technologische Einheitlichkeit zu bewahren, können damit aber auch Funktionen im Internet, die Netzfunktionen wie Vermittlung bzw. Routing im oben herausgearbeiteten Sinne realisieren und funktional gleichgerichtet auf einer höheren logischen Ebene nachbilden, Dienste in Telekommunikationsnetzen sein.

Zusammenfassend ist deshalb festzuhalten, dass "Transportdienste" des Telekommunikationsrechts von Inhalten abstrahieren. Dies kann aber auch für logische Netze, die ihre spezifische Funktionalität in höheren Schichten entfalten, konstatiert werden. Dass diese Dienste mit ihrer Vermittlungsfunktion auf Applikationsebene betrieben werden und ein logisches Netz über einem logischen Netz errichten, ist den Zufälligkeiten des Softwaredesigns und der Anwenderbedürfnisse geschuldet. Funktional wird hier gleichgerichtet vom Inhalt der Kommunikation abstrahiert.

[16] Anderer Ansicht in Hinblick auf VoIP-Provider [Katko 2005, S. 190]

6.3.3 Doppelfunktionalität von Diensten

Abschließend hätte sich nach der Rechtslage bei Geltung des TDG noch die Frage gestellt ob im Hinblick auf die hier fraglichen Dienste ein Ausschluss aus dem Regulierungsrahmen des TK-Rechts nicht deshalb erfolgen muss, weil sie zuförderst der Inhaltsebene des Telemedienrechts zuzuordnen sind. Hier ist unter der Ägide des TMG aber von einer Doppelfunktionalität auszugehen. Einer randscharfen Abgrenzung bedarf es insofern nicht mehr. Verzeichnisserver, welche rein zu Vermittlungszwecken genutzt werden, sind nicht zur menschlichen Wahrnehmung bestimmt und werden vom Nutzer so auch nicht wahrgenommen. Insofern verbleibt es bei der exklusiven Zuordnung zum Telekommunikationsrecht. Applikationen, die hingegen Inhalte vorhalten oder zwischenspeichern, sind insoweit wegen des unmittelbaren Inhaltsbezuges auch dem Telemedienrecht zuzuordnen.

6.3.4 Qualifizierungsmaßstäbe und Klassifizierung

Für die Qualifikation der hier streitigen Vermittlungsdienste, insbesondere der P2P-basierten, als Telekommunikationsdienst ergeben sich in der Zusammenfassung der technischen Voraussetzungen der Definition des Telekommunikationsdienstes in Zusammenschau mit dem Netzbegriff des TKG unter der Prämisse einer funktionalen Gleichrichtung der Tätigkeiten mit Dienstfunktionen in klassischen Telekommunikationsnetzen damit die folgenden Grundanforderungen:

- Sowohl die das Adress- bzw. Nummernschema realisierende Anwendungen der Endgeräte als auch der vermittelnde Dienst müssen im Rahmen einer gemeinsamen Protokollfamilie ein gemeinsames Adressierungsschema zum Verbindungsaufbau oder auf Ebene der Adressierung von einzelnen Datenpaketen bei der Übertragung der digitalen Signale verwenden.
- Dem vermittelnden Dienst muss dabei für den konkreten Kommunikationsvorgang die Funktion der Verwaltung des Adressraumes auf der Ebene des für die Verbindungssteuerung gewählten Protokolls zukommen. Unter Verwaltung des Adressraumes ist dabei das Angebot der administrativen oder technischen Zuweisung einer Nummer aus einem eigenen Nummernraum zu einem Endgerät oder Nutzer zu verstehen.
- Da Telekommunikationsdienst und Netzbetrieb aber, wie oben ausgeführt, nach der gesetzlichen Intention auch auseinander fallen können, ist alternativ auch die Auflösung einer eigenen oder fremden Nummer zu einer Nummer der tiefer liegenden Basiskommunikation hinreichend.

Insofern sollen im Folgenden einzelne Dienste in Overlay-Netzen sowohl nach den unstreitigen Kriterien der Dienstdefinition als auch insbesondere im Hinblick

auf ihre Vermittlungsfunktion nach den zuvor ermittelten Konkretisierungsmaßstäben eingeordnet werden. Um die Widerspruchsfreiheit zu belegen, muss sich die Betrachtung dabei auch auf Dienste des klassischen Internet erstrecken.

Overlay Kommunikation in der Internet Indirection Infrastructure (i3): Im Rahmen der Internet Indirection Infrastructure (i3) werden Datenpakete anhand einer flachen hierarchielosen Kennung ID einem Endsystem auf paketvermittelnde Weise zugestellt. Die verwendeten IDs können von den Systemen selbst gewählt werden. Der Verwaltung, genauer der Registrierung der IDs in i3 selbst (in i3 als Trigger bezeichnet), kommt eine entscheidende Rolle zu, da nur so die Zuordnung zwischen i3-ID und aktueller IP-Adresse stattfinden kann. Aufgrund des expliziten Routing jedes einzelnen Datenpakets spricht man auch von "late binding", da die Kennung im i3-Netz erst "spät" mit der schlussendlichen IP-Adresse abgebildet wird [Balakrishnan et al. 2004, S. 350].

Das i3 erweist sich, aufgrund seines eigenen Adressschemas und der betriebsnotwendigen Verwendung auf den Endsystemen und Zwischenknoten der Kommunikation, als Telekommunikationsnetz. Knotenfunktionalitäten, die die Registrierung der IDs und das Routing der Datenpakete leisten, sind bei Erfüllung der ökonomischen Kriterien als Telekommunikationsdienste einzuordnen.

Skype: Fraglich ist hingegen, ob Verzeichnisdienste bei VoIP-Applikationen als Telekommunikationsdienste anzusehen sind. Hier findet regelmäßig keine Durchleitung auf dem Vermittlungsserver statt. Mittels der fallweisen Auflösung des adressierungsrelevanten Benutzernamens könnte aber gleichwohl eine unabdingbare Voraussetzung für den eigentlichen Kommunikationsakt auf logische Ebene geschaffen werden. Bei der Inanspruchnahme des Dienstes ist zunächst eine Registrierung erforderlich, bei der eine Koordinierung des Skype-eigenen Adressierungsschemas vorgenommen wird. Beim eigentlichen Kommunikationsvorgang muss dieser Benutzername aufgelöst und der jeweils aktuellen IP-Adresse des Nutzers zugeordnet werden. Die eigentliche Verbindung kann damit nur durch vorgeschaltete Übermittlung der relevanten Adressinformationen, bestehend aus Skype-Namen und zur Laufzeit zugeordneter IP-Adresse des Empfängers der Kommunikation, stattfinden. Dieses Namensschema ist sodann auch für den Verbindungsaufbau beim eigentlichen Kommunikationsvorgang unverzichtbar. Insofern sind die Voraussetzungen für die Annahme eines virtuellen Telekommunikationsnetzes auch hier gegeben. Erst in der Folge findet sodann die eigentliche Sprachkommunikation ausschließlich auf IP-Ebene statt. Damit ist aber das Routing der eigentlichen das Sprachsignal repräsentierenden Datenpakete ohne vorgeschaltete Adresszuweisung und -auflösung nicht möglich. Das Skype-

System bzw. die es realisierenden Systeme leisten also eine mittelbare Steuerung im vorgenannten Sinne.

Im Gegensatz zu i3 findet im Fall von Skype eine frühe Zuordnung des Skype-Namens zur aktuellen IP-Adresse statt ("early binding", vgl. [Balakrishnan et al. 2004, S. 350]), nämlich vor Beginn der eigentlichen Kommunikation. Zukünftig sind auch andere Dienste denkbar, die Adresszuweisungen anbieten. Dabei werden dann Resolution Service Provider (RSP) neben den ISPs eine zentrale Rolle spielten [Balakrishnan et al. 2004, S. 349].

Es ist daher mit anderen Stimmen in der Literatur davon auszugehen, dass Skype als Telekommunikationsdienst anzusehen ist (vgl. auch [VAT, S. 2]). Dabei kann im Ergebnis aber auf die dargelegten, objektiven technischen Aspekte abgestellt werden, womit es nicht auf subjektive Sicht der Nutzer oder Anbieter für die Zuordnung ankommt[17].

BitTorrent: BitTorrent ermöglicht die effiziente Verbreitung von großvolumigen Inhalten wie bspw. Software-Distributionen oder Filmen. Da die beteiligten Knoten des P2P-Systems gleichzeitig die Dateien beziehen und wieder bereitstellen, folgt daraus eine effiziente Nutzung der vorhandenen Ressourcen. Die Ermittlung/Vermittlung der Knoten, die den Inhalt bereitstellen erfolgt entweder über einen zentralen Tracker-Server oder im Trackerless Modus durch ein P2P-Netz. Die Vermittlungsfunktion des so genannten Trackers bzw. die ihn ersetzenden Funktionalität im P2P-Netz, besteht dabei aus der Auflösung des im verwendeten Namensschema enthaltenen Dateinamens zu der IP-Adresse des die Dateien speichernden Client.

Das vorliegen eines virtuellen Telekommunikationsnetzes und in der Folge bei Vorliegen der ökonomischen Kriterien auch eines Telekommunikationsdienstes ist zu bejahen, da die Bezeichnungen der Dateien auf den Endgeräten als Nummern im Sinne von § 3 Nr. 13 TKG zu qualifizieren sind und der Tracker die Auflösung dieser Namen zu den jeweilig einschlägigen IP-Adressen vornimmt.

Da der Tracker gleichzeitig auch eine inhaltsbezogene Funktionalität realisiert, ist von einer Doppelfunktionalität auszugehen. Insofern ist auch das TMG einschlägig. Da daneben die einzelnen Peers auch Inhalte anbieten, sind die Betreiber in dieser Funktionalität in jedem Falle als Telemedien zu qualifizieren. Dabei ist zu beachten, dass nach § 5 Abs. 1 TMG hinsichtlich der Informationspflichten der Anwendungsbereich des Gesetzes ebenfalls von der Entgeltlichkeit des Angebotes abhängt (vgl. hierzu Abschnitt 6.5).

[17] Anderer Ansicht [Seitlinger & Strobl 2005, S. 9]

E-Mail-Dienste auf Basis von SMTP-Servern: Auch SMTP-Server sind als Vermittlungssysteme vor diesem Hintergrund als Telekommunikationsdienste einzuordnen. Auf diesen Servern fallen die Signalübertragung auf der physikalischen Schicht und die Bestimmung der Ziele der Datenpakete zusammen. Dabei werden die Netzabschlusspunkte des virtuellen Netzes auf Anwendungsebene gebildet. Es findet ein zusammengesetztes Namensschema Anwendung. Zum einen die Adressierung auf IP- bzw. Domainnamen-Ebene, welche eine Übertragung bis zum Endgerät erlaubt. Zum anderen wird ein virtuelles Netz für die eigentliche Ende-zu-Ende Kommunikation auf Anwendungsebene gebildet. In letzterem findet das vom Betreiber des SMTP-Servers verwaltete Namenschema Anwendung. Insofern ist auch diese für die Einordnung als virtuellen Telkommunikationsnetzes erforderliche Funktionalität gegeben. Soweit in der Begründung zum TMG-Entwurf [TMG-E] "E-Mail" global auch dem Telemedienrecht zugeordnet wird, kann sich diese Ausführung nur auf etwaige Webmail-Applikationen beziehen. Dies entspricht auch der in Erwägungsgrund 10 der RRL vorgenommenen differenzierteren Wertung. Die ausdrückliche Erwähnung der E-Mail-Übertragungsdienste zielt gerade auf SMTP-Server ab.

Domain Name System (DNS): Die Frage nach der Stellung des DNS muss hingegen differenziert beurteilt werden. Soweit der durch den Domainnamen gekennzeichnete Host auf einem, eine Vielzahl von Domains anbietende Server eingerichtet ist, kann der Domainname auch technisch zwingend adressierungsrelevant werden. Dies kann bspw. beim http- oder SMTP-Protokoll der Fall sein[18]. Der durch die IP-Adresse gekennzeichnete Abschlusspunkt des IP-Netzes reicht hier nicht zwangsläufig aus, um die gewünschte Kommunikation zu initiieren. Vielmehr muss der Domainname mit übertragen werden, um den zuständigen "virtuellen Server" anzusprechen. Insofern ist in diesem Fall das Bestehen eines virtuellen Telekommunikationsnetzes oberhalb IP zu bejahen. Da aber allein auf Ebene des Domainnamens keine Verbindung zum Zielrechner hergestellt werden kann und DNS-Server die Auflösung des Domainnamens zum Adressschema der tieferliegenden Basiskommunikation durchführen, sind sie in diesem Fall als Telekommunikationsdienst zu qualifizieren. Da das DNS gleichzeitig auch informatorischen Charakter besitzt, sind aber zugleich die Regelungen des Telemedienrechts einschlägig.

Problematisch könnte hingegen der Fall der Adressierung eines Endsystems sein, welcher nicht eine Vielzahl von Domains hostet. Hier kennzeichnet auf den ersten Blick die IP-Adresse den Netzabschlusspunkt für die gewünschte Übertragung der digitalen Signale hinreichend. Da in diesem Fall dem Domainnamen die

[18] Beim http findet hierzu der Host-Header-Eintrag Verwendung [RFC 2616, S. 128]

Funktion der Bezeichnung der Netzabschlusspunkte für den konkreten Kommunikationsvorgang fehlte, wäre das bestehen eines virtuellen Kommunikationsnetzes zu verneinen. Allerdings ist zu beachten, dass die Adresszuweisung aus einem einheitlichen Adressschema auf Seiten des Host schon vorgezogen vorgenommen worden ist. Durch Einträge in den DNS-Servern des für die Domain zuständigen NIC und des Hosters wird die Zuweisung des Domainnamens zu einer IP-Adresse zur Laufzeit erst ermöglicht. Die Einträge in den DNS-Servern sind insofern dem Endgerät zuzurechen. Ohne Adressauflösung ist wiederum die Verbindung zwischen dem, unter Verwendung eines Domainnamens, einen Kommunikationsvorgang auslösenden Client und dem Server nicht möglich. DNS-Server sind also in jedem Falle auch als Telekommunikationsdienste einzustufen.

Linklisten und Suchdienste: Linklisten im Internet dienen hingegen nicht der Adressierung in einem Telkommunikationsnetz. Die Zuweisung des "verlinkten" Namensraumes nach dem Schema *Domain oder IP-Adresse : Port / serverspezifische Kennung* (vgl. hierzu *Uniform Resource Identifier (URI)*-Schema [RFC 3986]) wird allein vom Anbieter der Kommunikation bestimmt. Für den Verbindungsaufbau und das Routing wird vom Suchdienst, wie zum Beispiel google oder A9, keine Funktion bereitgestellt.

6.3.5 Ergebnis

Es hat sich somit gezeigt, dass P2P-Systeme[19] vor dem Hintergrund des Ende-zu-Ende-Paradigmas auch als Telekommunikationsdienste zu qualifizieren sind. Dies folgt aus dem technologieneutralen Ansatz der europäischen Regulierung und der technisch funktionalen Gleichrichtung mit herkömmlichen Telekommunikationsdiensten. Hierzu bedarf es aber der Neubewertung von bislang quasi normvertretend aufgefassten technischen Referenzmodellen. Außerdem ist es sinnvoll notwendige, den Anwendungsbereich eingrenzende Korrektive nicht im Rahmen der Legaldefinition des Telekommunikationsdienstes in § 3 Nr. 24 TKG anzusiedeln, sondern dies im Rahmen der spezifischen Rechtsfolgenregelungen wie zum Beispiel § 110 TKG vorzunehmen.

Zusammenfassend ergibt sich somit folgender Leitsatz für die Klassifikation:

> *Infolge der in der Rahmenrichtlinie geforderten Technologieneutralität sind funktional gleichgerichtete Dienste in "klassischen" und "neuartigen" Netzwerken gleichartig zu behandeln. Unter der Maßgabe des Ende-zu-Ende-Paradigmas können insofern auch mittelbar (die Kommunikation) steuernde Systeme Telekommunikationsdienste erbringen.*

[19] und mithin auch Teilfunktionalitäten von NGNs

6.4 Leitlinien für die Entwicklung und den Betrieb von P2P-Systemen und -Netzen

In diesem Abschnitt werden zunächst P2P-Systeme mittels des gewonnen Einordnungsschemas sowie deren funktionalen Klassifikation eingeordnet. Ferner werden wesentliche Rechtsfolgen, d.h. Rechte und Pflichten, dargelegt, die sich aus der Einordnung eines Dienstes als Telekommunikationsdienst oder Telemediendienst ergeben. Abschließend erfolgt eine Bewertung der Rechtsfolgen in Form von Leitlinien für Entwickler, Betreiber und Nutzer.

6.4.1 Einordnung der funktionalen P2P-Klassen

Aus dem entwickelten Einordnungsschema nach dem Ende-zu-Ende-Paradigma ergibt sich die in Tabelle 6.1 dargestellte Einordnung der P2P-Systeme. Dabei wurden die Klassifikation gemäß Abschnitt 6.2.3 zugrunde gelegt. Weiterhin soll

P2P-Klasse	**TK-Dienst**	**Telemediendienst**
Lokalisierung von Nutzern bzw. Endsystemen und Vermittlung von Verbindungen	+	–
Lokalisierung von Inhalten bzw. Informationsdiensten	+	+
Weiterleitung von Datenpaketen	+	–
Bereitstellung von Inhalten	–	+

Tabelle 6.1: Einordnung von P2P-Systemen entsprechend ihrer Funktion

hier angemerkt werden, dass es sich um eine exemplarische Verortung handelt. Da eine solche Klassifikation nicht alle Aspekte eines konkreten P2P-Systems widerspiegeln kann, ist diese Einordnung als Leitlinie zu verstehen, ohne dabei die Verortung von spezifischen P2P-Systemen vorweg zu nehmen. Darüber hinaus kann auch die konkrete Verortung von P2P-Systemen aus Abschnitt 6.3.2 als Hilfe herangezogen werden.

6.4.2 Rechtsfolgen

Eine vollständige Darstellung von möglichen Rechtsfolgen für Telekommunikationsdienste und Telemedien verbietet sich an dieser Stelle, da hierzu ein konkreter Sachverhalt, d.h. ein zu beurteilendes P2P-System notwendig wäre. Die folgenden dargestellten Rechtsfolgen wurden in Hinblick darauf ausgewählt, dass sie sich telekommunikations- oder telemedienrechtlich motiviert unmittelbar auf die

Entwicklung und den Betrieb von gängigen P2P-Systemen und -Netzen auswirken können.

Unter den Randbedingungen gelten für Dienste in P2P-Systemen, die als Telekommunikationsdienste zu qualifizieren sind, unter anderem folgende Rechtsfolgen:

- Nach § 6 TKG ist die Aufnahme, Änderung und Beendigung des Betriebs von Telekommunikationsnetzen und -diensten der Bundesnetzagentur anzuzeigen werden, wenn diese für die Öffentlichkeit bestimmt sind und ein gewerblicher Betrieb erfolgt.
- Telekommunikation und somit auch Telekommunikationsdienste unterliegen dem Fernmeldegeheimnis gemäß § 88 TKG. Insofern müssen Betreiber dafür Sorge tragen, dass sowohl die Vertraulichkeit bei der Telekommunikation selbst gewahrt bleibt als auch die näheren Umstände der Telekommunikation wie Nummern vertraulich bleiben.
- Der Umgang mit personenbezogenen Daten im Rahmen von Telekommunikationsdiensten ist in § 91 ff. TKG geregelt und orientiert sich, hinsichtlich der im TKG nicht explizit geregelten Prinzipien, darüber hinaus an den gängigen Maßstäben[20] des Bundesdatenschutzgesetzes (BDSG) [BDSG 2003]. Um dem besonderen Schutzzweck des Fernmeldegeheimnis gerecht zu werden, werden im Gegensatz zu den Regelungen des BDSG dessen Schutzprogramm nur für natürliche Personen greift gemäß § 91 Abs. 1 TKG Einzelangaben die dem Fernmeldegeheimnis unterliegen bei juristischen Personen personenbezogenen Daten gleichgestellt.
- Aus technischer Sicht ist insbesondere auch § 109 zu berücksichtigen, in welchem vorgeschrieben ist, dass technische Vorkehrungen zu treffen sind, so dass das Fernmeldegeheimnis und der Datenschutz gewahrt bleiben. Werden die TK-Dienste für die Öffentlichkeit erbracht ist auch ein Sicherheitsbeauftragter zu benennen sowie ein Sicherheitskonzept zu erstellen.
- Betreiber von Telekommunikationsdiensten, die für die Öffentlichkeit bestimmt sind, müssen gemäß § 110 TKG technische Einrichtung vorhalten, um die Überwachung der Telekommunikation zu ermöglichen. Wenn eine Überwachung nur durch Zusammenwirken von mehreren Systemen möglich ist, sind hierfür automatisierte Steuerungsmöglichkeiten vorzuhalten. Dabei ist zu beachten, dass der Kreis der Verpflichteten durch § 3 der Telekommunikations-Überwachungsverordnung (TKÜV) [TKÜV 2005] eingeschränkt wurde. So müssen bspw. keine Vorkehrungen getroffen werden, wenn weniger als 10.000 Teilnehmer angeschlossen sind.

[20] insbesondere: Datenvermeidung und Datensparsamkeit (§3a BDSG) sowie technisch-organisatorische Schutzvorkehrungen (Anlage zu § 9 BDSG)

– Darüber hinaus müssen Betreiber von öffentlich zugänglichen Telekommunikationsdiensten gemäß § 113a TKG erzeugte und verarbeitete Verkehrsdaten für sechs Monate speichern. Dies trifft P2P-Netze jedoch nicht, da in den Abs. 2-4 einzelne Telekommunikationsdienste wie Telefondienste, elektronische Post und Internetzugangsdiensten explizit benannt sind.

Ferner gelten für Telekommunikationsdienste noch zahlreiche Rechtsfolgen in Hinblick auf die Abrechnung von Dienstleistungen, die Frequenzordnung und Marktregulierung, die jedoch nicht Gegenstand dieser Untersuchung sind, da sie keinen unmittelbaren Einfluss auf die technische Gestaltung von P2P-Systemen und -Netzen haben. Bei Telekommunikationsdiensten können sich zum Beispiel Regelungen zur Marktregulierung entsprechend § 9 ff. TKG eröffnen. Hierdurch erfolgt sodann die Umsetzung der entsprechenden europäischen Richtlinien, in welchen von den nationalen Regulierungsbehörden gefordert wird einen wirksamen Wettbewerb zu gewährleisten (vgl. Art. 8 RRL). Insofern müssen insbesondere transparente und nichtdiskriminierende Verfahren zur Frequenz- und Nummernvergabe etabliert werden. Ferner können Unternehmen mit beträchtlicher Marktmacht dazu verpflichtet werden zu fairen, ausgewogenen und nichtdiskriminierenden Bedingungen Mitbewerbern den Zugang zu ihren Diensten zu öffnen (vgl. Art. 5 der Zugangsrichtlinie).

Aus technischer Sicht gelten für Telemediendienste gemäß des TMG insbesondere folgende unmittelbaren Rechtsfolgen:

– Der Betrieb von Telemediendiensten ist gemäß § 4 TMG zulassungs- und anmeldefrei.
– Betreiber von Telemediendiensten sind nach § 5 TMG unter bestimmten Voraussetzungen verpflichtet allgemeine Informationspflichten, in der Regel umgangssprachlich als Impressum bezeichnet, zu erfüllen.

6.4.3 Entwickler-, Betreiber- und Nutzerleitlinien

Aus den dargelegten Rechtsfolgen können Leitlinien für Entwickler, Betreiber und Nutzer von P2P-Systemen abgeleitet werden (vgl. zu Rollen in P2P-Systemen Abschnitt 3.2.2), wie sie auch von der europäischen Kommission unter der Stichwort “security and privacy by design” nunmehr für sicherheitskritische Technikbereiche zunehmend gefordert werden [EU Kons 2008, S. 23].

Für Entwickler von P2P-Systemen beinhalten die Rechtsfolgen keine unmittelbaren Verpflichtungen. Jedoch kann durch entsprechende Gestaltung der Software der Betrieb letztlich vereinfacht werden.

Handelt es sich bei einem P2P-System um einen Telekommunikationsdienst, kann bspw. durch Verschlüsselung der übermittelten Daten, die Wahrung des

Fernmeldegeheimnis unterstützt werden. Aus Gründen des Datenschutzes dürfen im Allgemeinen auch keine personenbezogenen Daten gespeichert werden. Dies muss von Entwicklern insbesondere bei der Protokollierung der Kommunikation bedacht werden und müssen insofern die Grundsätze der Datenvermeidung und Datensparsamkeit gemäß § 3a des BDSG Anwendung finden.

Handelt es sich um einen Telemediendienst müssen gegebenenfalls allgemeine Informationspflichten erfüllt werden. Das System muss dabei dem Betreiber überhaupt die Möglichkeit geben werden dieser Verpflichtung nachzukommen. Da die Voraussetzungen einer gesonderten Betrachtung bedürfen, werden im folgenden Abschnitt 6.5 werden die Voraussetzungen und mögliche Realisierungen hierfür detailliert untersucht.

Für Betreiber ergeben sich die Leitlinien direkt aus den genannten Rechtssätzen ergebenden Rechtsfolgen. Dabei ist zu beachten, dass sowohl technische als auch organisatorische Maßnahmen nötig sind. Da die Umsetzung von organisatorischen Maßnahmen aufgrund der dezentralen Struktur von P2P-Systemen erschwert ist, sollten hierbei vor allem technische Vorkehrungen getroffen werden.

Wie im vorigen Abschnitt ausgeführt, sind bei dem Betrieb eines Telekommunikationsdienstes gegebenenfalls Schnittstellen vorzuhalten, um eine Überwachung der Kommunikation zu ermöglichen. Bei P2P-Systemen, die aus einer Menge von gleichartigen Peers bestehen, wird dies jedoch in der Regel nicht notwendig sein, da nicht mehr als 10.000 Peers[21] mit einem Peer verbunden sind. Existiert ein exponierter Betreiber (vgl. Abschnitt 3.2.2) wie zum Beispiel Skype kann bei diesem jedoch eine Verpflichtung zur Vorhaltung solcher Schnittstellen gegeben sein. Den Mangel an Überwachungsschnittstellen in solchen neuartigen Diensten führt unter anderem auch zu der Forderung von Ermittlungsbehörden nach so genannten Online-Durchsuchung [Hansen et al. 2007]. Durch die Installation einer speziellen Anwendung, einem so genannten Trojaner, wird hierbei die Überwachung der Ende-zu-Ende-Kommunikation ermöglicht. Da der Zugriff des Trojaners jedoch nicht auf einzelne Telekommunikationsdienste beschränkt werden kann, bleibt fraglich ob ein solches Mittel zulässig ist (so auch der Rechtsgedanke hinter der Entscheidung des Bundesverfassungsgerichts zum so genannten "IT-Grundrecht" [BVerfG 1 BvR 370/07]).

Typischerweise sind die Peer-Betreiber auch gleichzeitig Nutzer des P2P-Systems. Daher steht ihnen im Fall eines Telekommunikationsdienstes vor allem das Recht zu, dass die Kommunikation und die näheren Umstände vertraulich bleiben. Insofern dürfen weder exponierter Betreiber von P2P-Systemen noch private Peer-Betreiber unberechtigter Weise Einblick in, über ihren Rechner vermittelte, Daten nehmen. Hinsichtlich des Datenschutzes eröffnet sich lediglich durch

[21] Die Verpflichtung der TKÜV gilt nunmehr erst ab 10.000 Teilnehmeranschlüssen.

§ 100 TKG eine Ausnahme, der es Telekommunikationsdiensteanbietern gestattet zur Beseitigung von Störungen oder zur Feststellung von Missbräuchen bei konkretem Verdachtsmomenten eine Erhebung und Verarbeitung von Bestands- und Verkehrsdaten durchzuführen.

6.5 Telemedienrechtliche Informationspflichten in P2P-Systemen

Aus den dargestellten Leitlinien im vorigen Abschnitt geht hervor, dass P2P-Systeme, welche nicht ausschließlich als Telekommunikationsdienste im Sinne des TKG einzuordnen sind, gegebenenfalls allgemeine Informationspflichten erfüllen müssen. Diese Informationspflichten beinhalten bspw. den Namen und die Anschrift des Dienstbetreibers. Da jedoch nicht alle Dienste diese Angaben machen müssen, stellt sich die Frage für welche Arten von Diensten dies zutrifft und somit auch welche Gesetze einschlägig sind.

Die vormals notwendige Abgrenzung von Diensten gemäß Teledienstgesetz und Mediendienstestaatsvertrag hat sich nach der Novellierung des TMG zwar erübrigt, so dass auf der ersten Blick lediglich der § 5 des TMG relevant erscheint. Bei genauerer Betrachtung zeigt sich jedoch, dass solche Dienste auch in den Anwendungsbereich des Rundfunkstaatsvertrags (RStV) [RStV 2007] fallen können, da P2P-Systeme, wie in Abschnitt 2.4.4 gezeigt wurde, insbesondere auch zum Fernseh- und Video-Streaming genutzt werden.

Voraussetzung für das Eingreifen der allgemeinen Informationspflichten nach § 5 TMG bzw. § 55 RStV für Betreiber von Netzknoten und zentralen Instanzen ist, dass sie als Diensteanbieter einzuordnen sind. Nach der Legaldefinition des § 2 Nr. 1 TMG ist Diensteanbieter jede natürliche oder juristische Person, die geschäftsmäßig, in der Regel gegen Entgelt, eigene oder fremde Telemedien bereithält oder den Zugang zur Nutzung vermittelt. Nachdem mit der Novelle des TMG die zuvor in § 2 Abs. 2 TDG [TDG 97] enthaltenen Positivbeispiele wie Datendienste oder Telespiele entfallen sind, beurteilt sich die Einordnung eines Angebotes als Telemedium nur noch anhand der Negativliste des § 1 TMG. Für die Verortung des jeweiligen Dienstangebotes kommt es somit auf eine Negativabgrenzung zum Telekommunikationsdienst und zum Rundfunk an.

6.5.1 Abgrenzung zum Rundfunk

Wegen der unterschiedlichen Ausgestaltung insbesondere der Voraussetzungen des Eingreifens der Informationspflichten und dem Umfang der dann bereitzustellenden Informationen nach § 5 TMG und § 55 Abs. 1 RStV ist weiterhin auch

noch zwischen deren diesbezüglichen Anwendungsbereichen zu differenzieren (vgl. hierzu Abschnitt D.8 und D.4 im Anhang). Die Systematik des TMG und des neuen Rundfunkstaatsvertrages ist allerdings insofern nicht ganz klar. Von einigen Autoren wird daher auch der neue § 55 Abs. 1 RStV neben § 5 TMG als überflüssig erachtet, da es sich bei allen Internetdiensten im Grundsatz um Telemediendienste handele, sollen sich nach einer Auffassung die Informationspflichten primär nach § 5 Abs. 1 TMG richten [Hoeren 2007, S. 801, 803].

Diese Sicht wird aber den unterschiedlichen Schutzzwecken der Informationspflichten aus § 5 TMG und § 55 Abs. 1 RStV nicht gerecht. Die Informationspflichten des § 5 TMG haben auf Grund des Kompetenztitels einen wirtschaftsbezogenen Zweck [BR-Drs. 556/06, S. 12] und sichern insbesondere die Rechtsverfolgung und Transparenz der Nutzer bei Geschäftstätigkeiten im Zusammenhang mit Telemedien. Die Informationspflichten des § 55 Abs. 1 RStV folgen hingegen inhaltlich aus dem Wissen um das Herkommen von Filmbeiträgen, die Meinungsbildung beeinflussend sind [LT-Drs. 16/1046, S. 42]. Im Hinblick auf § 1 Abs. 4 TMG mit seinem Verweis auf die Geltung der inhaltsbezogenen Regelungen des RStV kann § 55 Abs. 1 bei Diensten ein eigenständiges Gewicht gewinnen, wenn es am Merkmal der Entgeltlichkeit des Telemediums mangelt, Inhalte mit meinungsbildender Funktion angeboten werden, der persönliche oder familiäre Bereich nach der Zwecksetzung des Angebotes aber verlassen wird.

6.5.2 Einordnung der Knotenfunktionalität ausgewählter P2P-Systeme

Im Hinblick auf VoIP-Dienste realisieren nach der hier vertretenen Auffassung die einzelnen Knotenrechner lediglich Funktionalitäten, die eine ausschließlich telekommunikationsrechtliche Verortung gebieten. Damit entfällt die Pflicht zur Bereitstellung der allgemeinen Pflichtinformationen nach dem TMG schon auf dieser Ebene. Die Darstellung der aufgelösten Klarnamen in der Suchoberfläche des Skype-Angebotes ist hingegen als telemedienrechtlich zu beurteilendes Informationsangebot zu werten.

Ebenso ist auch das Angebot einer P2P-Informationsverteilung bei Film-Verteildiensten differenziert zu bewerten. Neben den in diesen Overlay-Netzwerken enthaltenen telekommunikationsrechtlich zu würdigenden Teilaspekten, welche die Übermittlung oder Vermittlung der Inhalte betreffen, tritt der Bereitsteller der Inhalte, der konkrete Knoten, dem Endnutzer zwar nicht mit einem eigenen klassischen Telemediendienst, wie eine Website, gegenüber. Gleichwohl können die Knoten als Anbieter eigene oder fremde Telemedien zur Nutzung bereithalten. Das Bereithalten eigener Telemedien ist dann zu bejahen, wenn der Dienst, also

bspw. Video-on-Demand in einem eigenen Speicher vorgehalten wird [Roßnagel 2005, Waldenberger, zu § 3 TDG, Rn. 23]. In einem offenen Video-Verteilsystem, wie BitTorrent, in dem Inhalte von den Nutzern eingestellt werden, bieten die Nutzer Telemedien (den Video-on-Demand Dienst) an und halten ihn zur Nutzung bereit. Die Peers treten also als Anbieter eigener Telemedien auf.

Anders stellt es sich jedoch dar wenn das Dienstangebot auf einer Plattform basiert, bei welcher eine exponierter Betreiber existiert, die den Zugriff auf die Inhalte steuern kann. Ein solches System ist bspw. die Plattform in2movies [WWW In2movies]. Dabei stellen die Nutzer die abgerufenen Filme wiederum anderen Nutzern der Plattform bereit. Teilweise erhalten die Nutzer durch den Plattformbetreiber hierfür eine Vergütung in Form von Bonuspunkten. Der Nutzer betreibt insofern mit seinem Peer einen Teil der Infrastruktur. Die Sicherung der Inhalte sowie das Abrechnungsmanagement ist dabei zentralisiert und wird vom Plattformbetreiber vorgenommen, wobei die Rechtesicherung durch Digital Rights Management (DRM) stattfindet. Trotz vergleichbarer technischer Funktionalität der Peers ist bei solchen Dienstangeboten fraglich, ob die einzelnen Peer-Betreiber allgemeine Informationspflichten erfüllen müssen. Zwar sind bei oberflächlicher Sicht auch hier die Inhalte im Speicher der einzelnen Peers vorhanden. Zudem sind die bereitgestellten Inhalte zuvor vom Nutzer dieses Knotens auch anderweitig abgerufen worden und können von ihm betrachtet werden. Allerdings bedingt ein Zugriff auf diese Speicher durch die DRM-Sicherung der Inhalte eine Einschaltung des Plattformbetreibers.

Es stellt sich insofern die Frage, ob es sich deshalb in dieser Fallgestaltung des Video-on-Demand für die Peers nicht vielmehr um ein Angebot fremder Telemedien handelt. Dann müsste das konkrete Angebot allerdings dem Plattformbetreiber als eigener Telemediendienst zuzurechnen sein. Zwar kann dieser anders als beim klassischen Hosting-Dienst nicht nach belieben disponieren, was aber bei der Bereitstellung eines eigenen Telemediums auf einem Drittserver verlangt wird (vgl. [Manssen 2005, Brunner, zu § 3 TDG, Rn. 4] und [Roßnagel 2005, Waldenberger, zu § 3 TDG, Rn. 23]). Vielmehr hängt es vom Betreiber des Knotenrechners ab, welche Filme über sein System verfügbar gehalten werden und ob der Knoten überhaupt verfügbar ist. Auf der anderen Seite stellt der Knotenbetreiber hier kein vollständiges Angebot eines eigenen Video-on-Demand bereit, da die notwendigen Inhalte bei dieser Fallgestaltung durch den DRM-Schutz nicht ohne Mitwirkung des Plattformbetreibers genutzt werden können. Im Ergebnis wird das Knotenangebot aus technischer Sicht deshalb als eine Mischform aus Host- und Proxy-Provider für die Knotenfunktionalitäten und mithin das Angebot eines fremden Telemediums zu bejahen sein. Dieser Wertung entspricht es auch, dass die Haftungsprivilegierung des § 9 TMG für die Knotenbetreiber greift.

Schließlich muss für das Eingreifen der Informationspflichten nach § 5 Abs. 1 TMG das Angebot auch geschäftsmäßig, in der Regel gegen Entgelt erfolgen. Dies könnte auch bei mittelbarer Finanzierung[22] von VoIP-Angeboten wie Skype zu bejahen sein.

Bei der Filmdistribution im Rahmen eines offenen Video-Verteilsystems wie BitTorrent ist es eine Frage des Einzelfalles, ob für die Inanspruchnahme Entgeltlichkeit vereinbart ist. In Bezug auf die im Zusammenhang mit diesem Diensteangebot vielfältig aufgetretenen Verletzungen von Verwertungsrechten, erweist sich die telemedienrechtliche Neuregelung allerdings als ungerichtet. Gerade im Hinblick auf die durch Transparenzgebote ermöglichte Rechteverfolgung muss der Umweg über Auskunftsansprüche gegen Zugangsprovider gewählt werden, was zutreffend aus datenschutzrechtlichen Gesichtspunkten kritisiert worden ist [A-Drs. 16 9, Nr. 6 b)].

Ein vorzugswürdigerer Weg, die Interessen der Rechteverfolgung sowie des Schutzes der informationellen Selbstbestimmung in einen verhältnismäßigen Ausgleich zu bringen, wird hingegen im Rahmen des § 55 Abs. 1 RStV beschritten. Die Regelung greift die datenschutzrechtliche Terminologie des § 1 Abs. 2 Nr. 3 BDSG auf, womit auf die hierzu entwickelten Grundsätze zurückgegriffen werden kann. Zudem dient sie in ihrem abgestuften System der Informationspflichten gerade auch dem Zweck des Schutzes der informationellen Selbstbestimmung, wie sich aus der Begründung mit Blick auf die Freihaltung von persönlichen oder familiären Tätigkeiten aus der grundsätzlichen Informationspflicht ergibt [LT-Drs. 16/1046, S. 44]. In diesem Rahmen würde also die Teilnahme an einem offenen Video-Verteilsystem schon bei Überschreitung des persönlichen oder familiären Rahmens Informationspflichten auslösen, wohingegen im Kontext des § 5 TMG die Schwelle der Entgeltlichkeit überschritten sein müsste.

Sofern allerdings ein exponierter Betreiber als Anbieter gegenüber dem Nutzer auftritt, sind die einzelnen Peer-Betreiber trotz ihrer Diensteanbietereigenschaft nicht zu nutzergerichteten Informationen verpflichtet. Zwar werden grundsätzlich die einzelnen Knotenbetreiber bei diesem Geschäftsmodell vom Plattformbetreiber vergütet. Nach dem Schutzzweck des § 5 TMG scheidet aber die Verpflichtung zur Veröffentlichung der Pflichtinformationen aus. Gegenüber den Nutzern tritt ausschließlich der Plattformbetreiber als Vertragspartner und somit möglichen Anspruchsgegner bei der Rechteverfolgung auf.

[22] So ist bspw. die Kommunikation innerhalb des Skype-Netzes zwar kostenlos. Für die Kommunikation ins PSTN entstehen jedoch Kosten, so dass insgesamt eine Mischkalkulation und somit mittelbare Finanzierung zu unterstellen ist.

6.5.3 Realisierung der Pflichtinformationen

Weiterhin ist die Bewertung der Realisierung in Hinblick auf die unterschiedlichen Dienstgestaltungen nur differenziert vorzunehmen. Sofern P2P-Applikationen zur Anwendung kommen, mit welchen der Nutzer direkt interagiert und die von *einem* Betreiber angeboten werden, können entsprechende allgemeine Informationspflichten in die Software integriert werden. Bei diesen Diensten lassen sich die Merkmale "leichte Erkennbarkeit" und "unmittelbare Erreichbarkeit" analog zu einem so genannten *Anker für die Anbieterkennzeichnung (AKZ)* auf einer Homepage durch die Bereitstellung eines Reiters der jeweiligen Benutzeroberfläche verwirklichen, der beim Aufruf die geforderten Informationen anzeigt. Wird lediglich eine Schnittstelle für die Maschine-zu-Maschine-Kommunikation zu Verfügung gestellt, ergibt sich ein zusätzlicher Problemkreis, da der Bereitsteller keinerlei Einfluss auf die Darstellung nehmen kann. Diese Problematik wird zum Ende des Abschnitts vertieft betrachtet. Diese Gestaltung dürfte den Anforderungen entsprechen, die durch die Rechtsprechung zur Erkennbarkeit und Erreichbarkeit von Informationen durch das Setzen von so genannten *AKZ-Links* entwickelt wurden (vgl. u.a. [Schramm 2004, S. 472]). Der schon in der ursprünglichen Gesetzesbegründung zum TDG geforderten Maßgabe, dass "die Informationen ohne langes Suchen auffindbar sein müssen", wäre mit dieser Gestaltung genügt [BT-Drs. 14/6098, S. 21].

Problematisch könnten hingegen die Anforderungen des § 5 TMG an die ständige Verfügbarkeit der Pflichtinformationen in P2P-Systemen zu realisieren sein. Offensichtlich hat der Gesetzgeber und in der Folge auch die einschlägige Literatur im Hinblick auf dieses Merkmal primär eine Client/Server-Architektur vor Augen gehabt, bei der sich der Anbieter und somit auch der Server unter einer wohlbekannten Adresse immerwährend im Netz findet. Der Anbieter hat somit die Möglichkeit, die Informationen bei Bedarf abrufbereit zu halten. Insofern wird eine Sachverhaltsgestaltung wie die vorliegende, bei der systembedingt Peers nur temporär an dem System teilnehmen, in der Literatur regelmäßig nicht in den Fokus genommen.

In [Woitke 2003b, S. 873] wird in diesem Zusammenhang auf die Präsentation statt auf den nachwirkenden Gehalt des Merkmales abgestellt. So wird einerseits immerhin dargelegt, dass "ständig verfügbar" "überhaupt verfügbar" mit einschließe, jedoch nur, um darauf zu verweisen, dass dieses Kriterium bspw. bei dem Erfordernis eines Browser-Plugins zur Darstellung nicht erfüllt sei. Ein weiterer Autor leitet daraus ein Maß für die Erreichbarkeit der AKZ von einzelnen Seiten einer Homepage ab, da sie "ständig verfügbar" seien, wenn der Nutzer innerhalb des Web-Angebotes jederzeit auf sie zugreifen könne [Woitke 2003a, S. 946]. Andere Verfasser wollen das Merkmal als "Two-Click"-Erfordernis be-

greifen [Brunst 2004, S. 12]. Damit sei das Impressum jederzeit in Reichweite des Nutzers und damit ständig verfügbar. Aus systematischer Sicht ist dem entgegenzuhalten, dass das Tatbestandsmerkmal "unmittelbare Erreichbarkeit" keinen eigenständigen Regelungsgehalt mehr hätte. Neben den Kriterien "leicht erkennbar" und "unmittelbar verfügbar" enthält es vielmehr den Normappell, einen Zugang zu den Informationen nicht nur für den Zeitpunkt der eigentlichen Transaktion zu gewähren. Aus dem Schutzzweck der Norm ergibt sich, dass es einen dauerhaften Zugriff über diesen Zeitpunkt hinaus sichern soll. Eine mögliche Rechteverfolgung wird im Regelfall dem eigentlichen Geschäftsvorfall zeitlich nachgelagert einsetzen. Insofern würde die zwischenzeitliche Entfernung der Pflichtangaben eine entsprechende Verfolgung verhindern oder jedenfalls erschweren.

Erfüllung der Informationspflichten in "volatilen" P2P-Systemen: Da Peers nicht wie ein klassischer Web-Server dauerhaft unter einer wohlbekannten Adresse im Netz erreichbar sind, stellt sich die Frage, welche Anforderungen sich in P2P-Systemen im Hinblick auf das Merkmal der "ständigen Verfügbarkeit" ergeben. Bei enger Auslegung wäre eine Erfüllung durch Peers nach ihrer Struktur unmöglich.

Zu den Diensten der Informationsgesellschaft gehören ausweislich der Richtlinienbegründung aber auch gerade moderne, zurzeit der Gesetzgebung noch unbekannte Dienste, soweit sie die dort angesprochenen wirtschaftlichen Tätigkeiten unterstützen. Damit verhält sich die Richtlinie *technikneutral* und es ist bei der Auslegung zu berücksichtigen, dass vor diesem Hintergrund jedenfalls nichts technisch Unmögliches und dem Modell des P2P-Systems Zuwiderlaufendes zu fordern sein wird. Insofern ist es vertretbar, die Regelung nach ihrem Schutzzweck weit auszulegen und im Rahmen der Nutzung der Dienste einen Teil der Rechtesicherung in die Hände der Nutzer zu legen, soweit nur der Diensteanbieter das ihm technisch Mögliche getan hat. Die Ziele des Gesetzes, die Herstellung von Transparenz zur Rechteverfolgung und der Realisierung des Verbraucherschutzes, können auf diesem Wege gleichgut erreicht werden. Insofern müssen Dienste, welche nur auf einen unsteten Betrieb im Netz angelegt sind oder die über keine wohlbekannte Adresse verfügen, sicherstellen, dass die Informationen dem Empfänger zugänglich sind und von diesem abgespeichert werden können, so dass zu einem späteren Zeitpunkt die Informationen in Form einer lokalen Kopie zur Verfügung stehen.

Erfüllung der Informationspflichten im Rahmen der Maschine-zu-Maschine-Kommunikation: Der zweite Problemkreis bezieht sich auf Systeme, die nicht unmittelbar auf menschliche Wahrnehmung angelegt sind oder lediglich eine De-

finition der Maschine-zu-Maschine-Schnittstelle vorgenommen wurde. Fraglich hierbei ist wie allgemeine Informationspflichten gemäß TMG bzw. RStV in solchen Systemen erfüllt werden können. Bisherige Handhabungsverfahren beziehen sich auf Dienste, welche auf menschliche Wahrnehmung ausgelegt sind.

In der Literatur wird das Bereitstellen von Inhalten in der Regel als Telemediendienst im Sinne des TMG verstanden. Insofern sind bspw. Web Services (vgl. Abschnitt 4.1.2) ebenso einzustufen, da hier die Inhalte im Vordergrund stehen. Es handelt sich somit auch nicht um Telekommunikationsdienste im Sinne von § 3 Nr. 24 TKG. Im Fall des direkten Zugriffs auf einen Web Service handelt es sich primär um ein Darstellungsproblem. Insofern wäre in Analogie zur herkömmlichen Betrachtung klassischer Internet-basierter Dienste eine Angabe direkt im übermittelten XML-Konstrukt denkbar. Allerdings liegt die Darstellung nicht in Händen des Inhaltebereitstellers. Neben Web Services ergibt sich diese Problematik bei P2P-Systemen zusätzlich dahingehend, das offene Systeme wie BitTorrent, in welchen einzig die Maschine-zu-Maschine-Schnittstelle definiert wurde, die Entwicklung alternativer Clients zulassen, die ihrer Darstellung jedoch völlig unterschiedlich sind.

Der Dienstanbieter kann insofern die "leichte Erreichbarkeit" in diesen Fällen nicht gewährleisten, wenn man aus den Kriterien der "leichten Erkennbarkeit" und "unmittelbaren Erreichbarkeit" konkrete Gestaltungsanforderungen ableitet [LG Berlin 2002 2003], müsste zum Beispiel eine Realisierung eine gemeinsame und herausgehobene Interpretation der Daten erzwingen. Nun hat es aber der Bereitsteller der Inhalte nicht in der Hand, mit welcher Software die Daten dargestellt werden bzw. vielmehr weiterverarbeitet werden und kann insofern diese Anforderung niemals erfüllen. Es ist gerade das Wesen dieser neuen Datenstrukturen, die Darstellung und den Inhalt zu trennen. Legt man die Rechtsprechung des OLG Hamburg zum Mangel der Erreichbarkeit durch notwendiges "Scrollen auf Webseiten" an [OLG Hamburg 2002 2003], würde selbst die Möglichkeit der externen Betrachtung der XML-Strukturen hier nicht hinreichen.

Selbst wenn man sich insofern hinsichtlich der Schutzbedürftigkeit der Nutzer eher am Verbraucherleitbild des EuGH orientiert und nach der auf die Sicht des durchschnittlich informierten und verständigen Durchschnittsverbrauchers abstellt (vgl. u.a. [Woitke 2003a, S. 947]), kann aber die Wortlautgrenze nicht überschritten werden. Notwendig ist immer, dass die Informationen überhaupt erkennbar sind. Dies wird regelmäßig nicht möglich sein, sofern der Nutzer nicht über eine Software verfügt, die einen entsprechenden Interpretationsschritt für ihn leistet. Insofern kann nur der Gesetzgeber gefordert sein, in seine Überlegungen zur Ausgestaltung von Transparenzgeboten mehr Technologieneutralität einfließen zu lassen. Vorzugswürdig wäre es insofern, bei den Gestaltungsanfor-

derungen mit einem Erfüllungsauftrag nach dem "Stand der Technik" einen Weg für die Einbeziehung der Standardisierungen der IETF [WWW IETF] oder des W3C [WWW W3C] zu eröffnen und in der Folge die Erfüllung der Pflichten von der technisch möglichen Einhaltung von entsprechenden Auszeichnungen abhängig zu machen. Sofern dann der Verbraucher eine nicht standardkonforme Software zur Interpretation der Daten einsetzt, muss das Risiko in seiner Sphäre bleiben. Die Darstellung lässt sich somit zwar nicht beeinflussen, aber durch Standardisierung der Informationsstrukturen könnte man den Schutzzweck des § 5 TMG gleichgut erreichen. Dabei ist es möglich, eine Realisierung so vorzunehmen, dass für die allgemeinen Informationspflichten eine "Standard-XML-Anfrage" festgelegt wird und die Web Services mittels einer standardisierten Informationsstruktur antworten.

6.5.4 Ergebnis

Dienste, die durch P2P-Systeme realisiert werden, können auch dem Regulierungsregime des TMG und mithin den Informationspflichten des § 5 TMG zuzurechnen sein. Wie gezeigt wurde, kommen teilweise aber auch die Informationspflichten gemäß § 55 RStV in Betracht. Tabelle 6.2 gibt hierzu nochmals eine zusammenfassende Übersicht. Dem in P2P-Systemen auftretenden inhärenten Problem der Fluktuation der Peers kann durch eine weite Auslegung des Begriffs der ständigen Verfügbarkeit begegnet werden und es wird insofern eine proaktive Sicherung der Informationen beim Nutzer vorgeschlagen.

	Telemediendienst gemäß	
Art des Dienstes	**TMG**	**RStV**
entgeltlich & meinungsbildend	+	+
nicht entgeltlich & meinungsbildend	–	+
entgeltlich & nicht meinungsbildend	+	–
nicht entgeltlich & nicht meinungsbildend	–	–

Tabelle 6.2: Zu erfüllende Informationspflichten je nach Art des Dienstes

Im Gegensatz zum WWW ist bei P2P-Systemen oder allgemeiner bei Nutzung von Maschine-zu-Maschine-Schnittstellen ist wegen der Trennung von Inhalt und Darstellung die Erfüllung von konkreten Gestaltungsanforderungen der allgemeinen Informationspflichten, wie sie in den letzten Jahren von Literatur und Rechtssprechung entwickelt wurden, für den Diensteanbieter unmöglich. Im ersten Schritt wäre hierfür eine Standardisierung der Pflichtinformation zielführend, um den Anwendungsentwicklern somit die Möglichkeit zu geben die Informationen in angemessener Weise darzustellen.

6.6 Zusammenfassung

In diesem Kapitel wurden ausführlich die Herausforderungen erläutert, welche bei der Einordnung von P2P-Netzen und -Systemen im telekommunikationsrechtlichen Rahmen entstehen. Dabei wurde vor allem die Problematik bei der Abgrenzung von Telekommunikationsdiensten gemäß TKG und Telemedien gemäß TMG verdeutlicht.

Da sich bestehende Einordnungsschemata als nicht tragfähig erwiesen, wurde in der Folge ein neues Einordnungsschema entwickelt, in welchem durch eine interdisziplinäre Betrachtung die Kriterien der beiden Fachdisziplinen der Rechtswissenschaften sowie der Informatik miteinander in Einklang gebracht wurden. Das Schema basiert dabei auf dem Ende-zu-Ende-Paradigma und ermöglicht insbesondere, die notwendige Technikneutralität zu wahren. Mittels dieses Einordnungsschemas ergibt sich letztlich auch die telekommunikationsrechtliche Verortung von P2P-Systemen und -Netzen. Bedingt durch das breite Anwendungs- und vor allem Funktionsspektrum von P2P-Systemen kann dabei keine allgemeine Zuordnung vorgenommen werden. Es wurden jedoch Kriterien aufgezeigt, anhand derer eine Zuordnung stattfinden kann. Eine Zuordnung wurde sodann auch exemplarisch für existierende P2P-Systeme vorgenommen.

Im zweiten Teil des Kapitels wurden ausgewählte Rechtsfolgen, welche sich aus der jeweiligen Zuordnung ergeben, dargelegt. Ein Kernelement bei Telemedien sind die allgemeinen Informationspflichten. Da diese Informationspflichten nicht von jedem Diensteanbieter zu erfüllen sind und sich bei P2P-Systemen auch die technischen Realisierung als problembehaftet erweist, wurden hierzu passende Lösungen entwickelt.

Sowohl bei dem entwickelten Einordnungsschema als auch den Lösungen zur Realisierung von allgemeinen Informationspflichten bildeten zwar P2P-Systeme den Ausgangspunkt. In beiden Bereichen konnten jedoch Lösungen gefunden werden, die in einem breiteren Anwendungsbereich wie zum Beispiel Next-Generation-Networks oder auch bei Web Services nutzbringend eingesetzt werden können.

7
Zusammenfassung

P2P-Systeme und die darin enthaltenen P2P-Netze werden mittlerweile von Millionen Nutzern gleichzeitig verwendet und verursachen mehr als 50 % des Datenvolumens im Internet. Das Anwendungsspektrum reicht dabei von Dateitauschbörsen über Sprachtelefoniedienste bis hin zu universellen Verzeichnisdiensten. Davon ausgehend war es das Ziel der Arbeit, das Potential von P2P-Netzen und -Systemen für zukünftige Systeme und Netze näher zu beleuchten.

Im ersten Teil der Arbeit erfolgte eine umfassende Darlegung der Hintergründe und des aktuellen Entwicklungsstandes. Hierzu wurden sowohl abstrahierte Definitionen und Unterscheidungsmerkmale wie das P2P-Ebenenmodell als auch konkrete Ausprägungen von P2P-Netzen und Systemen wie Kademlia und BitTorrent präsentiert. Die Arbeit gibt hiermit einen Überblick über das Themengebiet und bietet dem Leser durch zahlreiche referenzierte Arbeiten die Möglichkeit zur weiteren Vertiefung.

In der Folge wurde der aktuelle Stand der Entwicklung bezüglich im Internet eingesetzter Systeme, wissenschaftlicher Arbeiten und Standardisierungsbemühungen dargelegt sowie eine Charakterisierung von P2P-Systemen vorgenommen. Dabei zeigte sich, dass P2P-Systeme sowohl aus Sicht des Netzwerks als auch der verteilten Systeme eine Virtualisierungstechnologie darstellen. Aus Netzsicht ergeben sich neuartige logische Netze, die insbesondere ergänzende Adressierungsmöglichkeiten eröffnen. Hinsichtlich verteilter Systeme wird, in Ergänzung zu der funktionalen Separierung von Multi-Tier-Architekturen, eine Abstrakti-

onsebene zwischen Diensten und konkreten Rechnersystemen etabliert, die eine selbstorganisierende und dynamische Lastverteilung ermöglicht.

Aus der Charakterisierung des aktuellen Entwicklungsstandes ergab sich weiterhin, dass P2P-Systeme für dedizierte Anwendungsbereiche mit vielen Teilnehmern gut geeignet sind. Ferner wurden jedoch auch folgende offene Fragen identifiziert, die im weiteren Verlauf der Arbeit näher analysiert wurden:

1. Integration von P2P-Netzen in bestehende verteilte Systemarchitekturen
2. Eignung von P2P-Techniken für Systeme mit wenigen Teilnehmern
3. Robustheit von P2P-Systemen hinsichtlich Angriffen
4. Telekommunikationsrechtliche Verortung von P2P-Systemen und -Netzen

1. P2P-Systeme sind für dedizierte Anwendungsgebiete gut geeignet und die Architekturen daher meist monolithisch gestaltet. Man spricht auch von einer guten vertikalen Integration. Es stellte sich jedoch die Frage, ob P2P-Techniken auch in komplexen verteilten Systemen wie einer elektronischen Marktplattform zum Einsatz kommen können. In dieser Arbeit konnte durch die Konzeption von so genannten ServiceNets und einer entsprechenden Knotenarchitektur eine *dienstorientierte P2P-Architektur* realisiert werden, die eine Diensterbringung durch mehrere Knoten auch in komplexen verteilten Systemen ermöglicht. Die Architektur basiert dabei auf einer Kombination von Web Services und P2P-Netzen in Form von Modulen, die insbesondere eine Entkopplung von Anwendungsdiensten und P2P-Netzen ermöglichen und somit P2P-Techniken horizontal integrieren. Ferner erlaubt die Architektur den parallelen Einsatz von mehreren P2P-Netzen, so dass die Auswahl des P2P-Netzes je nach Dienstanforderungen erfolgen kann. Insgesamt eröffnet diese Architektur P2P-Systemen somit ein wesentlich breiteres Einsatzspektrum.

2. In zahlreichen Systemen ist die Eignung von P2P-Systemen für Millionen von Teilnehmern zu beobachten. Fraglich blieb bislang allerdings, inwiefern P2P-Systeme für Systeme mit wenigen Teilnehmern, so genannte Mikro-P2P-Systeme, geeignet sind. Nachteilig bei Mikro-P2P-Systemen ist, dass die Skalierbarkeit von P2P-Systemen hinsichtlich vieler Teilnehmer nicht zum Tragen kommt und für den Beitritt zu einem P2P-System, das so genannte Bootstrapping, meist zentrale Komponenten zum Einsatz kommen. Durch die Entwicklung einer kollaborativen Architektur, welche ein weit verbreitetes P2P-System mit vielen Teilnehmern zum Bootstrapping nutzt, in Verbindung mit einer dezentralen Knotensuche konnten diese Nachteile ausgeräumt werden und das Einsatzspektrum von P2P-Systemen somit auch auf Systeme mit wenigen Teilnehmern ausgedehnt

Analyse	Art	Abschnitt
Knotendichte und Sitzungsdauer von BitTorrent-DHT-Knoten	Messung	4.2.4
Optimierung der zufälligen Adressprüfung bei der Knotensuche	analytisch	4.2.5
Fehlertoleranz von P2P-Systemen	analytisch	5.2
Ressourcenverbrauch eines BitTorrent-DHT-Knotens	Messung	5.5.1
Einfluss von Sybils bei Kademlia-Netzen (inklusive Routing-Table-Poisoning)	simulativ	5.5.2
Limitierung der Sybil-Anzahl durch Bandbreitenbeschränkung	simulativ	5.6.1

Tabelle 7.1: Ausgewählte Analysen und Bewertungen dieser Arbeit

werden. Die Tragfähigkeit der Konzepte wurde durch empirische Messungen hinsichtlich Knotendichte und Sitzungsdauer von Knoten in der BitTorrent-DHT und entsprechende wahrscheinlichkeitstheoretischen Analysen aufgezeigt. Zusätzlich konnte durch eine analytische Bewertung die Knotensuche optimiert werden. Darüber hinaus wurde ein Verfahren für ein *optimiertes Probing durch filterresistente Port-Selektion* vorgeschlagen, welches die Knotensuche in zukünftigen P2P-Systemen wesentlich beschleunigt.

3. Bei P2P-Systemen erwiesen sich insbesondere die Dezentralität und die damit einhergehenden selbstorganisierenden Mechanismen als vorteilhaft, da hierdurch ein hoher Grad an Fehlertoleranz erreicht werden kann. In der Arbeit wurde diese Fehlertoleranz bei der Datenhaltung und dem Routing in P2P-Systemen mittels einer analytischen Bewertung ausführlich dargelegt. Kommt es zu gezielten Angriffen bösartiger Knoten, kann diese Fehlertoleranz teilweise unterminiert werden, so dass der Robustheitsgrad des Gesamtsystems beschränkt bleibt. Dabei stellte sich der sogenannte Sybil-Angriff als äußerst effektiv heraus, bei welchem ein Angreifer unter mehreren Identitäten im System agiert und somit Redundanzmechanismen aushebeln kann. Bekannte Abwehrstrategien sind dabei nicht ausreichend bzw. nur in bestimmten Kontexten anwendbar, da sie entweder eine zentrale Entität oder externe Vertrauensbeziehungen zwischen den Peers verlangen. Ziel der Arbeit war es insofern zu evaluieren, inwieweit die Ressourcenbeschränkungen eines Angreifers möglichst effektiv für die Beschränkung der Anzahl Sybils genutzt werden können. Daher wurde zunächst eine ressourcenbasierte Analyse anhand eines Kademlia-Netzes durchgeführt, woraus hervorging, wie viele

Verfahren	Abschnitt
Dienstorientierte P2P-Architektur	4.1
Optimiertes Probing durch filterresistente Port-Selektion	4.2.7
Selbstregistrierung	5.6.2
Künstlicher Churn	5.6.3
Telekommunikationsrechtliches Einordnungsschema	6.3.5

Tabelle 7.2: Übersicht der in der Arbeit präsentierten neuartigen Verfahren

Ressourcen in Form von Netzwerkbandbreite, Rechenleistung und Speicherverbrauch für den Betrieb eines Knotens nötig sind, wobei sich die Netzbandbreite als limitierender Faktor erwies. Ferner wurde der Einfluss, den Sybils in einem Netz ausüben können, mittels Simulationen aufgezeigt. Dabei wurde insbesondere auch die katalysierende Wirkung von Routing-Table-Poisoning deutlich. Auf diesen Analysen basierend wurden verschiedene Abwehrstrategien entworfen und mittels simulativer Studien bewertet. So kann zum einen die Netzbandbreite als limitierender Faktor genutzt werden, indem die "Ping-Rate", d.h. die Frequenz, in welcher die Nachbarknoten kontaktiert werden und antworten müssen, variiert wird. Durch das neuartige *Verfahren zur Selbstregistrierung* wurde außerdem die Möglichkeit geschaffen, die Anzahl der Knoten pro IP-Adressbereich beliebig zu begrenzen. Ferner konnte durch die Einführung von *künstlichem Churn* die Sybil-Resistenz erhöht werden. Anhand der durchgeführten Analysen kann somit das Bedrohungspotential von Sybil-Angriffen abgeschätzt werden und zukünftige P2P-Systeme können unter Anwendung der aufgezeigten Abwehrstrategien robuster gegenüber solchen Angriffen gestaltet werden.

4. Aus betrieblicher Sicht müssen neben technischen auch rechtliche Aspekte bedacht werden. Bisherige rechtliche Analysen im Rahmen von P2P-Systemen fokussierten fast ausschließlich auf urheberrechtliche Gesichtspunkte in Dateitauschbörsen. Um das Potential von P2P-Techniken zu ergründen, muss jedoch auch eine telekommunikationsrechtliche Einordnung vorgenommen werden, da ansonsten die Rechte und Pflichten eines Peer-Betreibers nicht bestimmt werden können. Die Herausforderung bestand insbesondere in der korrekten Einordnung von P2P-Netzen in das bestehende Rechtssystem, da rechtliche Regelungen vor dem Hintergrund von typischen Client/Server-Systemen gestaltet wurden. Die umfassende technisch-rechtliche Analyse der relevanten gesetzlichen Regelungen auf nationaler sowie europäischer Ebene zeigte, dass existierende Einordnungsschemen für P2P-Systeme, aber auch für weitere zukünftige Netze wie

Next-Generation-Networks, ungeeignet sind. Insofern wurde ein neues *telekommunikationsrechtliches Einordnungsschema* entwickelt, durch welches die Einordnung von P2P-Systemen in den Rechtsrahmen wesentlich erleichtert wird. Hierzu wurde vor allem der Begriff des virtuellen Netzes hinsichtlich seiner Bedeutung und des resultierenden Anwendungsbereiches in semantischer, systematischer, historischer und teleologischer Hinsicht analysiert. Dabei konnte gezeigt werden, dass durch die Beurteilung der Dienstfunktionalitäten nach dem Ende-zu-Ende-Paradigma ein Einbezug mittelbar steuernder Systeme wie Verzeichnisdienste geboten ist und somit P2P-Systeme ganz oder in Teilen auch als Telekommunikationsdienste zu verorten sind. Aus dem entwickelten Schema wurden Leitlinien für Entwickler und Betreiber von Knoten abgeleitet. Außerdem wurden Konzepte zur Erfüllung von telemedienrechtlichen Informationspflichten in P2P-Systemen dargelegt.

Insgesamt eröffnet die vorliegende Arbeit der P2P-Technologie ein wesentlich breiteres Einsatzspektrum, indem die vorhandenen Verfahren und Mechanismen bewertet und in Kontext gesetzt, sowie durch die Ergänzung mit neuartigen Verfahren bestehende Defizite ausgeglichen wurden. Eine Übersicht der maßgeblichen Analysen der Arbeit wird in der Tabelle 7.1 gegeben, wobei die Bewertung je nach Eignung durch realweltliche Messungen, Simulationen und analytische Betrachtungen stattfand. Weiterhin sind in Tabelle 7.2 die neuartigen Verfahren zusammengefasst, die im Rahmen dieser Arbeit entwickelt wurden.

Zukünftig können P2P-Techniken somit gewinnbringend in massiv verteilten Umgebungen wie dienstorientierten Systemarchitekturen genutzt werden. Dabei wird vor allem der Robustheit von P2P-Systemen unter dem Einfluss von Angriffen bösartiger Knoten eine zunehmende Bedeutung zu kommen, da nur bei ausreichender Robustheit ein ausgedehnter Einsatz möglich ist. In diesem Sinne kann in weiteren Arbeiten die Anwendbarkeit der P2P-Mechanismen in spezifischen Anwendungsbereichen wie zum Beispiel dem Netzwerkmanagement oder dem so genannten Cloud-Computing vertieft untersucht werden. Darüber hinaus kann eine Weiterentwicklung der entworfenen Verfahren auf Basis der gewonnen Erkenntnisse erfolgen. So können unter anderem weitere P2P-Netze hinsichtlich ihrer Sybil-Resistenz untersucht werden und die Mechanismen in einem Feldtest angewendet werden. Ferner können die Arbeiten zu künstlichem Churn vertieft werden und bspw. eine Optimierung von nötiger Bandbreite im Verhältnis zur resultierenden Resistenz durchgeführt werden. Bei den telekommunikationsrechtlichen Ergebnissen kann einerseits die Einbringung der Erkenntnisse im Rahmen der Fortentwicklung des rechtlichen Rahmens erfolgen. Andererseits kann durch die Weiterentwicklung der formulierten Leitlinien in Form von Best-Practices die Realisierung von rechtskonformen P2P-Systemen forciert werden.

A

Zufällige Adressprüfung – Limitierung durch NAT-Router

A.1 Einleitung

Bei der zufälligen Adressprüfung, wie sie in Abschnitt 4.2 beschrieben wurde, wird die Suchrate durch die zur Verfügung stehende Upstream-Bandbreite begrenzt. Außerdem kann eine Limitierung der Suchrate durch zwischengeschaltete Systeme wie NAT-Router entstehen. Nimmt man eine Suchrate von 100 pkt/s und eine Paketgröße von 107 Byte an, ergibt sich eine benötigte Upstream-Bandbreite von ca. 86 kbit/s. In Experimenten zeigte sich jedoch, dass je nach Implementierung des NAT-Router bereits geringere Suchraten Probleme bereiten.

NAT-Router nehmen eine Abbildung der internen (in der Regel privaten) IP-Adresse und des entsprechenden Ports auf eine externe IP-Adresse und nebst Port vor. Der NAT-Router pflegt hierzu eine Verbindungstabelle, wie in Abb. A.1 dargestellt. Einkommende Datenpakete werden nur dann akzeptiert, wenn ein entsprechender Eintrag in der Verbindungsstabelle eingetragen ist. Dabei ist zu beachten, dass die meisten NAT-Router aus Sicherheitsgründen nur externe Datenpakete von IP-Adressen akzeptieren, zu denen zuvor ein Datenpaket geschickt wurde. In Abb. A.1 wird dies exemplarisch durch die Verbindung 5 dargestellt, welche zurückgewiesen wird. Inaktive Verbindungen werden nach Ablauf eines Timeout aus der Verbindungstabelle entfernt.

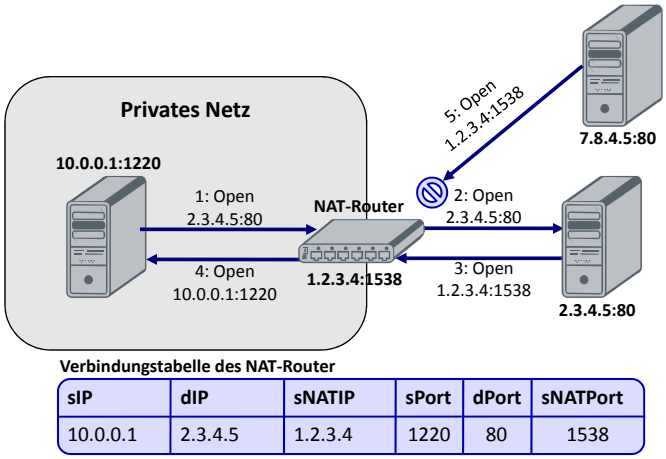


Abbildung A.1: Typisches Einsatzszenario eines NAT-Router

Problematisch bei der zufälligen Adressprüfung ist die Tatsache, dass für jede Prüfung ein Eintrag in der Verbindungstabelle angelegt werden muss, d.h. eine Suchrate von 100 pkt/s ist gleichzusetzen mit 100 neuen Einträgen in der Verbindungstabelle pro Sekunde. Insofern stellt sich die Frage, ob es zu einem Überlauf der Verbindungstabelle kommt und was die Folgen sind.

A.2 Überlauf von Verbindungstabellen

Für NAT-Router existieren keine verbindlichen Standards, sondern nur (informelle) Empfehlungen [RFC 2663]. Daher sind allgemein gültige Aussagen kaum zu treffen [RFC 3489]. Im Folgenden wird die Problematik daher anhand von drei exemplarisch ausgewählten NAT-Routern verdeutlicht:

- AVM FRITZ!Box Fon WLAN 7050, Firmware-Version: 14.04.33
- Linksys WRT54GL, Firmware-Version: OpenWrt WhiteRussion V. 0.9
- Netgear TA612V, Firmware-Version: 1.2_71

Das Verhalten beim Überlaufen von Verbindungstabellen ist unterschiedlich, je nach Implementierung des NAT-Routers wird die Tabelle in einer Art "Round-Robin-Verfahren" überschrieben (z.B. Netgear TA612V) oder es kommt zu Überlastungen des Routers (z.B. AVM FRITZ!Box und Linksys WRT54GL).

A.2.1 Überschreiben der Verbindungstabelle in NAT-Routern

Kommt es zu einem vorzeitigen überschreiben von Einträgen der Verbindungstabelle entsprechend des "Round-Robin-Verfahrens" bleiben die Einträge kürzer

als sonst üblich erhalten. Für die Suche nach einem DHT-Knoten bedeutet dies: Antwortet ein Peer nicht schnell genug, wird es unter Umständen nicht entdeckt, da das Antwortpaket vom NAT-Router verworfen wird.

Um die Größe der Verbindungstabelle zu ermitteln, wurde eine Menge Verbindungsinformationen $\{v_0, v_1, \ldots, v_k : v_i \neq v_j \text{für } i \neq j \text{ und } k \in \mathbb{N}\}$ generiert. Mittels jeder Verbindungsinformation wurde ein UDP-Paket versendet und anschließend wurde untersucht, ob noch eine Verbindung zu v_0 aufgebaut werden kann. Um die Anzahl der Tabelleneinträge zu ermitteln, kann k solange erhöht werden, bis eine Verbindung zu v_0 nicht mehr möglich ist. Versuche mit dem NAT-Router Netgear TA612V haben gezeigt, dass dieser 4.096 Tabelleneinträge in der Verbindungstabelle vorsieht.

Durch Festlegen einer maximalen Paketumlaufzeit RTT (engl. Round-Trip-Time, RTT) und der Anzahl der Tabelleneinträge TE ergibt sich die maximale Suchrate zu $\frac{TE}{RTT}$ Nimmt man 1 Sekunde als maximale Paketumlaufzeit folgt für den Netgear NAT-Router $s = \frac{4096\,\text{Einträge}}{1\,\text{sec}} = 4096\,\text{pkt/s}$. Bei einer Paketgröße von 107 Byte begrenzt der NAT-Router die Suchrate erst bei einer Upstream-Bandbreite von mehr als 3,3 Mbit/s.

A.2.2 Überlastung von NAT-Routern

Durch die Überlastung von NAT-Routern treten vermehrt Paketverluste an der WAN-Schnittstelle auf. Auf einigen NAT-Routern wie der AVM FRITZ!Box 7050 kommt es schließlich zu einem Komplettausfall, so dass keinerlei Pakete vom NAT-Router mehr verarbeitet werden.

Um den Zusammenhang zwischen Suchrate und UDP-Paketverlusten darzulegen, wurden beim genannten Linksys NAT-Router alle versendeten UDP-Pakete der WAN-Schnittstelle mitprotokolliert und mit der Anzahl versendeter Pakete an der internen LAN-Schnittstelle des NAT-Routers verglichen. Wie in Abb. A.2 dargestellt, zeigt sich dabei, dass der Anteil erfolgreich versendeter UDP-Pakete ab einer Suchrate von 50 pkt/s abnimmt. Bei 100 pkt/s beträgt der Paketverlust schließlich 50 %.

Da für die Ermittlung des Anteils erfolgreich versendeter UDP-Pakete ein Zugriff auf die WAN-Schnittstelle nötig ist, wurde ein Indikator gesucht, mittels dessen die Paketverluste auch von der internen LAN-Schnittstelle eingeschätzt werden können. Dabei erwies sich die Ermittlung von Paketumlaufzeiten mittels ICMP-Echo-Paketen als zielführend. Abb. A.2 zeigt auch diesen Zusammenhang auf. Dabei ist deutlich erkennbar, dass der Anteil von Paketverlusten und die erhöhte Paketumlaufzeiten korrelieren.

In Abb. A.3 sind unterschiedliche Versuchsläufe mit dem Linksys und AVM NAT-Router dargestellt. Daraus wird deutlich, dass bei der AVM FRITZ!Box 7050

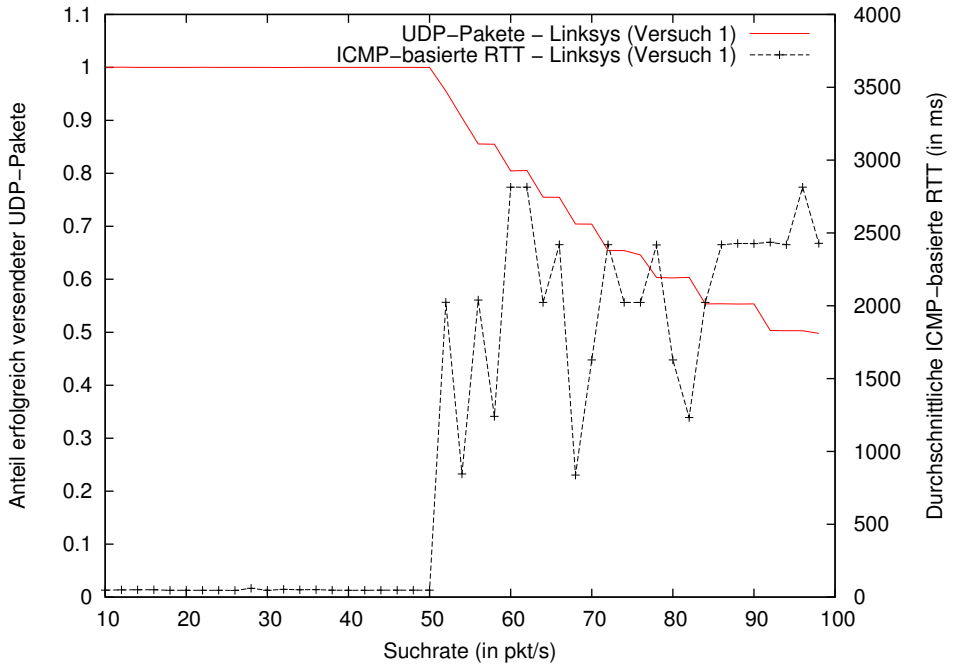


Abbildung A.2: Zunehmende UDP-Paketverluste bei ansteigender Suchrate im Vergleich zur ICMP-basierter Paketumlaufzeit

ab einer Rate von ca. 40 pkt/s mit Paketverlusten zu rechnen ist. Bei dem NAT-Router Linksys WRT45GL tritt dieser Effekt ab einer Rate von ca. 50 pkt/s auf. Für die Messungen wurden 300 Sekunden lang UDP-Pakete mit der angegebenen Suchrate versendet. Anschließend wurde eine Pause von 300 Sekunden eingelegt. In dieser Zeit kehrte der Router in den Normalzustand zurück und Verbindungen waren wieder möglich. Die Upstream-Bandbreite betrug dabei mindestens 200 kbit/s. Nicht beantwortete ICMP-Echo-Pakete wurden mit 4 Sekunden (dem entsprechenden Ping-Timeout) eingerechnet.

Das beobachte Verhalten schränkt die maximale Suchrate deutlich ein. Eine Suchrate von 40 pkt/s entspricht bei einer Paketgröße von 107 Byte in etwa einer Upstream-Bandbreite von 34 kbit/s. Legt man einen typischen DSL-Anschlusses mit einer Upstream-Bandbreite von mehr als 200 kbit/s zugrunde, wird die Suchrate in diesem Fall ausschließlich durch die Kapazitäten des NAT-Routers begrenzt.

Um etwaige NAT-Router nicht zu überlasten, kann die erhöhte Paketumlaufzeit als Indikator genutzt werden und die Suchrate adaptiv angepasst werden.

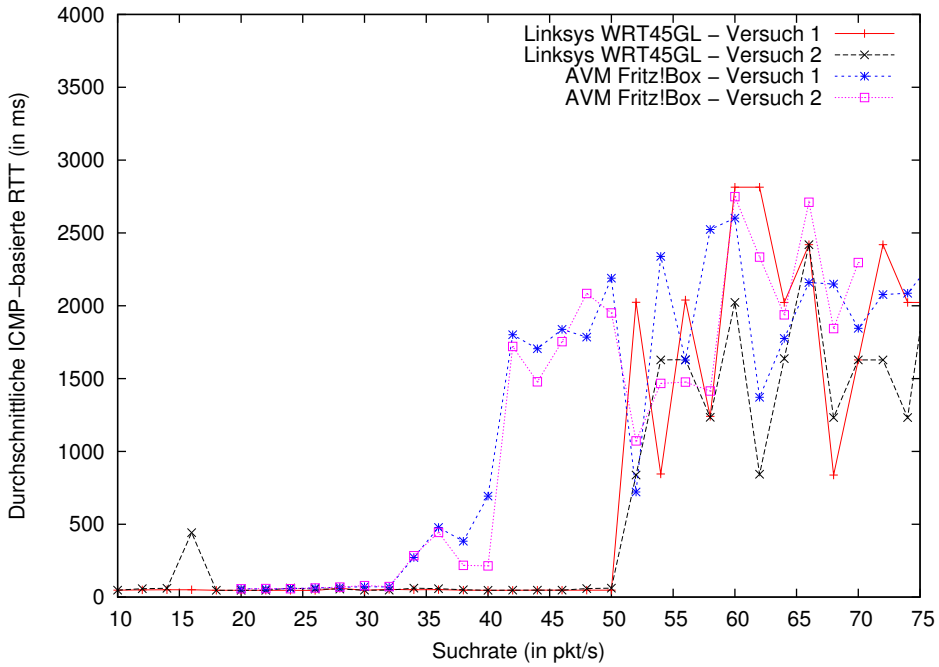


Abbildung A.3: ICMP-basierte Paketumlaufzeit im Verhältnis zur Suchrate

A.2.3 Firewalls

Letztlich betrifft diese Limitierung nicht nur NAT-Router, sondern auch Paket-filternde Firewalls, welche ein Connection Tracking durchführen (vgl. zu Firewalls u.a. [Dinger & Hartenstein 2008, S. 258]). Beim Connection Tracking werden auch Verbindungstabellen angelegt, so dass sich eine gleichgeartete Problematik ergibt. So zeigte sich bei der Durchführung der Messungen, dass die eingesetzte Firewall der Fakultät für Informatik der Universität Karlsruhe (TH) nicht mehr als 150 neue Verbindungen/s[1] von *einer* IP-Adresse verarbeiten kann.

A.3 Zusammenfassung

Die exemplarische Untersuchung von drei NAT-Routern zeigt, dass die maximale Suchrate durch die Verbindungstabelle in NAT-Routern begrenzt ist. Die Auswirkungen sind dabei abhängig von der spezifischen Implementierung des NAT-Routers. Teilweise führt dies bereits bei geringen Suchraten von 40 pkt/s zu Paketverlusten, so dass die maximale Suchrate im Wesentlichen durch den NAT-Router und nicht durch die Upstream-Bandbreite begrenzt werden. Da Paket-filternde Firewalls auch Verbindungstabellen führen, tritt das Problem dort auch auf.

[1] Stand: September 2007

B

Exkurs: Identität in elektronischen Systemen

B.1 Identitätsdefinitionen

In einem mathematischen algebraischen Sinne kann Identität wie folgt definiert werden:

> *"Identität ist eine Gleichheitsbeziehung zwischen zwei algebraischen Ausdrücken, die beim Einsetzen beliebiger Zahlenwerte anstelle der darin aufgeführten Buchstabensymbole erhalten bleibt."*
> aus [Bronstein et al. 1997, S. 8]

Dies ist jedoch nur eine Definition von Identität. Andere wissenschaftliche Disziplinen verwenden durchaus unterschiedliche Identitätsdefinitionen, obwohl der Kern der Definitionen – die Aussage über die Gleichheit bzw. Unterscheidbarkeit zweier Dinge (bzw. Personen) – allen Definitionen zugrunde liegt.

In der physischen Welt wird Identität in der Regel auf eine natürliche Person und letztlich deren Körper zurückgeführt. So verkürzt es J. Donath in [Donath 1998] auf die These *"The norm is: one body, one identity."* mit Bezug auf J.-P. Sartres These *"ich* bin *mein Körper, insofern ich* bin" [Sartre 1943, S. 577].

Auch das Verständnis von Identität im Sinne des Datenschutzrechts weist in die gleiche Richtung. So definiert die europäische Datenschutzrichtlinie in Art. 2

[EU 95/46/EG], dass die Identität einer natürlichen Person durch ein oder mehrere Elemente zum Ausdruck gebracht wird, die sie in ihrem physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Umfeld auszeichnen.

Im Rahmen dieser Arbeit und des Sybil-Angriffs ist vor allem der Bereich des Identitätsmanagements von Belang, da man sich dort intensiv mit dem Begriff der *elektronischen* bzw. *digitalen Identität* befasst. Eine Übersicht zu Forschungsprojekten, Standardisierungsinitiativen und gesetzlichen Regulierungen im Bereich Identitätsmanagement findet sich unter anderem in [Bramhall et al. 2007]. Dabei zeigt sich, dass sich sowohl Forschungsprojekte als auch Normierungsinstitutionen mit der Definition des Begriffs Identität auseinander setzen.

Stellvertretend sei hier die Definition des Projekts Prime angeführt, in welchem Identität als Symbol bzw. Menge an Symbolen aufgefasst wird, die sich auf eine Entität beziehen und eine Unterscheidung der Entitäten in einem spezifischen Kontext erlauben [EU Prj Prime, S. 13]:

> *"Identity: A symbol or a set of symbols referring to an entity, i.e. a subject or an object, allowing to distinguish it from others in a specific scope. The identifier could be a name which is imposed by a third party, being unique in a specific namespace."*
> aus [EU Prj Prime, S. 13]

Die bedeutende Normierungsinstitution ITU (International Telecommunication Union) ist gegenwärtig noch im Normierungsprozess im Rahmen der Identity Management Global Standards Initiative begriffen [WWW IdM-GSI]. Doch bereits die aktuelle Arbeitsdefinition weist in eine ähnliche Richtung:

> *"For ITU-T purposes, the identity asserted by an entity represents the uniqueness of that entity in a specific context and is not intended to indicate positive validation of a person. Identity management (IdM) is the process of secure management of identity information (e.g., credentials, identifiers, attributes, and reputations)."*
> aus [WWW IdM-GSI]

Aus diesen beiden Definitionen geht hervor, dass eine (elektronische) Identität immer nur in einem spezifischen Kontext definiert ist. Insofern gilt für die folgende Betrachtung:

> Eine Entität ist durch ihre Identität in einem spezifischen Kontext eindeutig bestimmt, d.h. es gelte eine 1-zu-1 Beziehung zwischen Entität und Identität in einem spezifischen Kontext.

B.2 Identität im Kontext des Sybil-Angriffs

Ziel dieses Abschnitts ist es, unter Berücksichtigung der vorgenannten Identitätsdefinition die Definition eines Sybil-Angriffs gemäß Douceur zu verfeinern.

Legt man die obige Identitätsdefinition zugrunde, kann eine Entität im gleichen Kontext nicht mehrere Identitäten erzeugen, da es das Wesen der Identität ist, eine Entität eindeutig auszuzeichnen. Insofern ist die Definition von Douceur wie folgt zu erweitern. Es handelt sich dann um einen Sybil-Angriff, wenn es einer Entität aus dem Kontext A gelingt, in einem Kontext B mehr als eine Entität zu besitzen bzw. zu erzeugen.

Die Generierung der Entitäten und Identitäten im Kontext B kann dabei entweder durch den Einsatz von Ressourcen erfolgen oder durch eine Abbildung der Identitäten, wie zum Beispiel durch eine Hash-Funktion. So können bspw. die menschlichen Fähigkeiten (vgl. CAPTCHA in Abschnitt 5.5) oder Rechenressourcen eingesetzt werden, um eine Entität wie ein E-Mail-Nutzerkonto im Kontext B zu generieren. Eine Abbildung von Identitäten erfolgt bspw. dann, wenn auf Basis einer Kreditkartennummer, die als Identität im Kontext A dient, eine Identität im Kontext B wie ein PayPal-Nutzerkonto erzeugt wird.

In Abb. B.1 sind die Zusammenhänge nochmals dargestellt, wobei es sich um einen Sybil-Angriff handelt, da es zu einer Entität aus dem Kontext A mehrere Entitäten und Identitäten im Kontext B gibt.

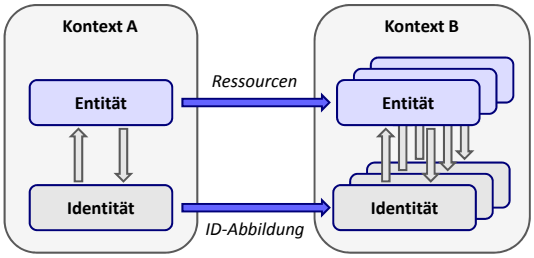


Abbildung B.1: Zusammenhang zwischen Entitäten und Identitäten

Wendet man dies nun auf den Sybil-Angriff in P2P-Systemen an, so ergibt sich der Kontext B zu: Der Kontext sei der Kontext P2P-System. Daraus folgt, dass die Entität einem Knoten entspricht und die Identität der P2P-Identität, was im Regelfall die Knotenkennung ist.

Trotz der Erweiterung von Douceurs Definition ist hinsichtlich der Frage, welche Annahmen für die Entitäten und Identitäten im Kontext A gelten, bislang wenig gewonnen.

Problematisch dabei ist insbesondere, dass *eine* Entität im Allgemeinen so viele digitale Entitäten und somit auch Identitäten generieren kann, wie sie bereit ist

Energie bzw. Ressourcen dafür zu investieren[1] [Donath 1998, S. 29].

> *"One can have, some claim, as many electronic personas as one has time and energy to create."*
> aus [Donath 1998, S. 29]

Für die ressourcenbasierte Analyse des Sybil-Angriffs in Abschnitt 5.5 wird daher ein zusätzlicher Kontext eingeführt, wie in Abb. B.2 dargestellt. Bei einem Sybil-Angriff versucht ein Angreifer, der einer Entität im Nutzerkontext entspricht, mittels seiner Rechner zu mehreren Entitäten im P2P-Kontext zu gelangen. Die Modellierung der Rechner als eigener Kontext ergibt sich daraus, dass bei einer ressourcenbasierten Limitierung der Sybils eine Identifikation nur auf dieser Ebene stattfinden kann. Anders würde es sich beim Einsatz sozialer Netze verhalten, da dort ein direkter Bezug zum Nutzerkontext etabliert wird. Rechner ist dabei stellvertretend für die IT-Ressourcen Rechenleistung, Speicherplatz und Netzwerkkapazitäten zu verstehen.

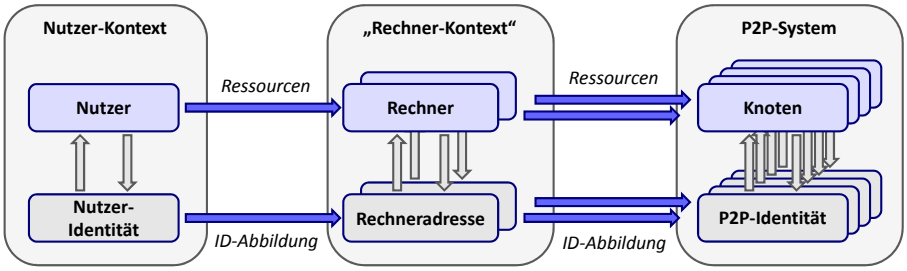


Abbildung B.2: Zusammenhang zwischen Entitäten und Identitäten bei der ressourcenbasierten Analyse eines Sybil-Angriffs

Aus Gründen der Lesbarkeit wurde in Kapitel 5 die verkürzende Schreibweise von Entität und Identität beibehalten, bei welcher der Kontext nicht explizit Erwähnung findet. Eine Identität im Sinne von Kapitel 5 ist somit als Identität im Kontext P2P-System und eine Entität im Nutzer-Kontext zu verstehen.

[1] Eine Ausnahme hierzu bilden Strukturen, wie sie durch eine Public Key Infrastructure (PKI) etabliert werden. Im Falle einer PKI wird der Bezug zwischen Identität und natürlicher Person durch die Registration Authority hergestellt.

C

Zusammenschau der mathematischen Symbole

Symbol	Bedeutung	Abschnitt
n	Anzahl der Knoten eines P2P-Netzes bzw. -Systems	2.4
m	Anzahl der Nachbarknoten eines Knotens, d.h. die Anzahl der Knoten in der Routing-Tabelle eines Knotens	5.2.2
h	Anzahl der Hops in einem Kommunikationspfad	5.2.2
a	Anzahl der IP-Adressen, die potentiell für den Betrieb von Knoten in Betracht kommen	4.2.4
b	Anzahl möglicher Ports, unter welchen ein Knoten betrieben werden kann	4.2.4
k	Versuchsanzahl bei der zufälligen Adressprüfung	4.2.4
l	Anzahl der zu überprüfenden Ports pro IP-Adresse bei der zufälligen Adressprüfung	4.2.4
d	Anzahl der disjunkter Kommunikationspfade	5.2.2
r	Anzahl der redundanten Knoten bei der Speicherung eines Datums	5.2.2
f	Anteil fehlerhafter Knoten / Ausfallwahrscheinlichkeit	5.2.2
$h(x)$	Konsistente Hash-Funktion wie SHA-1	4.2.7

Tabelle C.1: Übersicht der mathematischen Symbole, die in der Arbeit kapitelübergreifend Verwendung finden.

D

Auszüge aus telekommunikationsrechtlichen Regelungen

Für die telekommunikationsrechtliche Verortung in Kapitel 6 sind die Definitionen und Festlegungen der einschlägigen Gesetze und Richtlinien entscheidend. Insofern werden im Folgenden Auszüge aus den relevanten Gesetzen und Richtlinien dargelegt, die für das Verständnis notwendig sind:

D.1 Auszug aus dem deutschen Telekommunikationsgesetz (TKG)

Stand: Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 2 des Gesetzes vom 21. Dezember 2007 (BGBl. I S. 3198) [TKG 2004]

§ 1 Zweck des Gesetzes

Zweck dieses Gesetzes ist es, durch technologieneutrale Regulierung den Wettbewerb im Bereich der Telekommunikation und leistungsfähige Telekom-

munikationsinfrastrukturen zu fördern und flächendeckend angemessene und ausreichende Dienstleistungen zu gewährleisten.

§ 3 Begriffsbestimmungen

...

13. **"Nummern"** Zeichenfolgen, die in Telekommunikationsnetzen Zwecken der Adressierung dienen;

...

18. **"Rufnummer"** eine Nummer, durch deren Wahl im öffentlichen Telefondienst eine Verbindung zu einem bestimmten Ziel aufgebaut werden kann;

...

22. **"Telekommunikation"** der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen;

...

24. **"Telekommunikationsdienste"** in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen;

...

27. **"Telekommunikationsnetz"** die Gesamtheit von Übertragungssystemen und gegebenenfalls Vermittlungs- und Leitwegeinrichtungen sowie anderweitigen Ressourcen, die die Übertragung von Signalen über Kabel, Funk, optische und andere elektromagnetische Einrichtungen ermöglichen, einschließlich Satellitennetzen, festen und mobilen terrestrischen Netzen, Stromleitungssystemen, soweit sie zur Signalübertragung genutzt werden, Netzen für Hör- und Fernsehfunk sowie Kabelfernsehnetzen, unabhängig von der Art der übertragenen Information;

...

§ 6 Meldepflicht

(1) Wer gewerblich öffentliche Telekommunikationsnetze betreibt oder gewerblich Telekommunikationsdienste für die Öffentlichkeit erbringt, muss die Aufnahme, Änderung und Beendigung seiner Tätigkeit sowie Änderungen seiner Firma bei der Bundesnetzagentur unverzüglich melden. Die Erklärung bedarf der Schriftform.

...

§ 9 Grundsatz

(1) Der Marktregulierung nach den Vorschriften dieses Teils unterliegen Märkte, auf denen die Voraussetzungen des § 10 vorliegen und für die eine Marktanalyse nach § 11 ergeben hat, dass kein wirksamer Wettbewerb vorliegt.

(2) Unternehmen, die auf Märkten im Sinne des § 11 über beträchtliche Marktmacht verfügen, werden durch die Bundesnetzagentur Maßnahmen nach diesem Teil auferlegt.

(3) § 18 bleibt unberührt.

§ 47 Bereitstellen von Teilnehmerdaten

(1) Jedes Unternehmen, das Telekommunikationsdienste für die Öffentlichkeit erbringt und Rufnummern an Endnutzer vergibt, ist verpflichtet, unter Beachtung der anzuwendenden datenschutzrechtlichen Regelungen, jedem Unternehmen auf Antrag Teilnehmerdaten nach Absatz 2 Satz 4 zum Zwecke der Bereitstellung von öffentlich zugänglichen Auskunftsdiensten und Teilnehmerverzeichnissen zur Verfügung zu stellen. Die Überlassung der Daten hat unverzüglich und in nichtdiskriminierender Weise zu erfolgen.

(2) Teilnehmerdaten sind die nach Maßgabe des § 104 in Teilnehmerverzeichnissen veröffentlichten Daten. Hierzu gehören neben der Nummer sowohl die zu veröffentlichenden Daten selbst wie Name, Anschrift und zusätzliche Angaben wie Beruf, Branche, Art des Anschlusses und Mitbenutzer, soweit sie dem Unternehmen vorliegen. Dazu gehören auch alle nach dem jeweiligen Stand der Technik unter Beachtung der anzuwendenden datenschutzrechtlichen Regelungen in kundengerechter Form aufbereiteten Informationen, Verknüpfungen, Zuordnungen und Klassifizierungen, die zur Veröffentlichung dieser Daten in öffentlich zugänglichen Auskunftsdiensten und Teilnehmerverzeichnissen nach Satz 1 notwendig sind. Die Daten müssen vollständig und inhaltlich sowie technisch so aufbereitet sein, dass sie nach dem jeweiligen Stand der Technik ohne Schwierigkeiten in ein kundenfreundlich gestaltetes Teilnehmerverzeichnis oder eine entsprechende Auskunftsdienstedatenbank aufgenommen werden können.

(3) Ergeben sich Streitigkeiten zwischen Unternehmen über die Rechte und Verpflichtungen aus den Absätzen 1 und 2, gilt § 133 entsprechend.

(4) Für die Überlassung der Teilnehmerdaten kann ein Entgelt erhoben werden; dieses unterliegt in der Regel einer nachträglichen Regulierung nach Maßgabe des § 38 Abs. 2 bis 4. Ein solches Entgelt soll nur dann einer Genehmigungspflicht nach § 31 unterworfen werden, wenn das Unternehmen auf

dem Markt für Endnutzerleistungen über eine beträchtliche Marktmacht verfügt.

§ 66 Nummerierung

(1) Die Bundesnetzagentur nimmt die Aufgaben der Nummerierung wahr. Ihr obliegt insbesondere die Strukturierung und Ausgestaltung des Nummernraumes mit dem Ziel, den Anforderungen von Endnutzern, Betreibern von Telekommunikationsnetzen und Anbietern von Telekommunikationsdiensten zu genügen. Die Bundesnetzagentur teilt ferner Nummern an Betreiber von Telekommunikationsnetzen, Anbieter von Telekommunikationsdiensten und Endnutzer zu. Ausgenommen ist die Verwaltung von Domänennamen oberster und nachgeordneter Stufen.

§ 88 Fernmeldegeheimnis

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

(4) Befindet sich die Telekommunikationsanlage an Bord eines Fahrzeugs für Seefahrt oder Luftfahrt, so besteht die Pflicht zur Wahrung des Geheimnisses nicht gegenüber der Person, die das Fahrzeug führt oder gegenüber ihrer Stellvertretung.

§ 91 Anwendungsbereich

(1) Dieser Abschnitt regelt den Schutz personenbezogener Daten der Teilnehmer und Nutzer von Telekommunikation bei der Erhebung und Verwendung dieser Daten durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an deren Erbringung mitwirken. Dem Fernmeldegeheimnis unterliegende Einzelangaben über Verhältnisse einer bestimmten oder bestimmbaren juristischen Person oder Personengesellschaft, sofern sie mit der Fähigkeit ausgestattet ist, Rechte zu erwerben oder Verbindlichkeiten einzugehen, stehen den personenbezogenen Daten gleich.

(2) Für geschlossene Benutzergruppen öffentlicher Stellen der Länder gilt dieser Abschnitt mit der Maßgabe, dass an die Stelle des Bundesdatenschutzgesetzes die jeweiligen Landesdatenschutzgesetze treten.

§ 100 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten

(1) Soweit erforderlich, darf der Diensteanbieter zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden.

(2) Zur Durchführung von Umschaltungen sowie zum Erkennen und Eingrenzen von Störungen im Netz ist dem Betreiber der Telekommunikationsanlage oder seinem Beauftragten das Aufschalten auf bestehende Verbindungen erlaubt, soweit dies betrieblich erforderlich ist. Das Aufschalten muss den betroffenen Gesprächsteilnehmern durch ein akustisches Signal angezeigt und ausdrücklich mitgeteilt werden.

(3) Soweit erforderlich, darf der Diensteanbieter bei Vorliegen zu dokumentierender tatsächlicher Anhaltspunkte die Bestandsdaten und Verkehrsdaten erheben und verwenden, die zum Aufdecken sowie Unterbinden von Leistungserschleichungen und sonstigen rechtswidrigen Inanspruchnahmen der Telekommunikationsnetze und -dienste erforderlich sind. Zu dem in Satz 1 genannten Zweck darf der Diensteanbieter die erhobenen Verkehrsdaten in der Weise verwenden, dass aus dem Gesamtbestand aller Verkehrsdaten, die nicht älter als sechs Monate sind, die Daten derjenigen Verbindungen des Netzes ermittelt werden, für die tatsächliche Anhaltspunkte den Verdacht der rechtswidrigen Inanspruchnahme von Telekommunikationsnetzen und -diensten begründen. Insbesondere darf der Diensteanbieter aus den nach Satz 1 erhobenen Verkehrsdaten und den Bestandsdaten

einen pseudonymisierten Gesamtdatenbestand bilden, der Aufschluss über die von den einzelnen Teilnehmern erzielten Umsätze gibt und unter Zugrundelegung geeigneter Missbrauchskriterien das Auffinden solcher Verbindungen des Netzes ermöglicht, bei denen der Verdacht einer Leistungserschleichung besteht. Die Daten der anderen Verbindungen sind unverzüglich zu löschen. Die Bundesnetzagentur und der oder die Bundesbeauftragte für den Datenschutz sind über Einführung und Änderung eines Verfahrens nach Satz 1 unverzüglich in Kenntnis zu setzen.

(4) Unter den Voraussetzungen des Absatzes 3 Satz 1 darf der Diensteanbieter im Einzelfall Steuersignale erheben und verwenden, soweit dies zum Aufklären und Unterbinden der dort genannten Handlungen unerlässlich ist. Die Erhebung und Verwendung von anderen Nachrichteninhalten ist unzulässig. Über Einzelmaßnahmen nach Satz 1 ist die Bundesnetzagentur in Kenntnis zu setzen. 4Die Betroffenen sind zu benachrichtigen, sobald dies ohne Gefährdung des Zwecks der Maßnahmen möglich ist.

§ 109 Technische Schutzmaßnahmen

(1) Jeder Diensteanbieter hat angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze

1. des Fernmeldegeheimnisses und personenbezogener Daten und
2. der Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe

zu treffen.

(2) Wer Telekommunikationsanlagen betreibt, die dem Erbringen von Telekommunikationsdiensten für die Öffentlichkeit dienen, hat darüber hinaus bei den zu diesem Zwecke betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen, und gegen äußere Angriffe und Einwirkungen von Katastrophen zu treffen. Dabei sind der Stand der technischen Entwicklung sowie die räumliche Unterbringung eigener Netzelemente oder mitbenutzter Netzteile anderer Netzbetreiber zu berücksichtigen. Bei gemeinsamer Nutzung eines Standortes oder technischer Einrichtungen hat jeder Betreiber der Anlagen die Verpflichtungen nach Absatz 1 und Satz 1 zu erfüllen, soweit bestimmte Verpflichtungen nicht einem bestimmten Betreiber zugeordnet werden können. Technische Vorkehrungen und sonstige Schutzmaßnahmen sind angemessen, wenn der dafür erforderliche technische und wirtschaftliche Aufwand in einem

angemessenen Verhältnis zur Bedeutung der zu schützenden Rechte und zur Bedeutung der zu schützenden Einrichtungen für die Allgemeinheit steht.

(3) Wer Telekommunikationsanlagen betreibt, die dem Erbringen von Telekommunikationsdiensten für die Öffentlichkeit dienen, hat einen Sicherheitsbeauftragten oder eine Sicherheitsbeauftragte zu benennen und ein Sicherheitskonzept zu erstellen, aus dem hervorgeht,

1. welche Telekommunikationsanlagen eingesetzt und welche Telekommunikationsdienste für die Öffentlichkeit erbracht werden,
2. von welchen Gefährdungen auszugehen ist und
3. welche technischen Vorkehrungen oder sonstigen Schutzmaßnahmen zur Erfüllung der Verpflichtungen aus den Absätzen 1 und 2 getroffen oder geplant sind.

Das Sicherheitskonzept ist der Bundesnetzagentur unverzüglich nach Aufnahme der Telekommunikationsdienste vom Betreiber vorzulegen, verbunden mit einer Erklärung, dass die darin aufgezeigten technischen Vorkehrungen und sonstigen Schutzmaßnahmen umgesetzt sind oder unverzüglich umgesetzt werden. Stellt die Bundesnetzagentur im Sicherheitskonzept oder bei dessen Umsetzung Sicherheitsmängel fest, so kann sie vom Betreiber deren unverzügliche Beseitigung verlangen. Sofern sich die dem Sicherheitskonzept zu Grunde liegenden Gegebenheiten ändern, hat der Betreiber das Konzept anzupassen und der Bundesnetzagentur unter Hinweis auf die Änderungen erneut vorzulegen. Die Sätze 1 bis 4 gelten nicht für Betreiber von Telekommunikationsanlagen, die ausschließlich dem Empfang oder der Verteilung von Rundfunksignalen dienen. Für Sicherheitskonzepte, die der Bundesnetzagentur auf der Grundlage des § 87 des Telekommunikationsgesetzes vom 25. Juli 1996 (BGBl. I S. 1120) vorgelegt wurden, gilt die Verpflichtung nach Satz 2 als erfüllt.

§ 110 Umsetzung von Überwachungsmaßnahmen, Erteilung von Auskünften

(1) Wer eine Telekommunikationsanlage betreibt, mit der Telekommunikationsdienste für die Öffentlichkeit erbracht werden, hat

1. ab dem Zeitpunkt der Betriebsaufnahme auf eigene Kosten technische Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation vorzuhalten und organisatorische Vorkehrungen für deren unverzügliche Umsetzung zu treffen,

1a. in Fällen, in denen die Überwachbarkeit nur durch das Zusammenwirken von zwei oder mehreren Telekommunikationsanlagen sichergestellt werden kann, die dazu erforderlichen automatischen Steuerungsmöglichkeiten zur Erfassung und Ausleitung der zu überwachenden Telekommunikation in seiner Telekommunikationsanlage bereitzustellen sowie eine derartige Steuerung zu ermöglichen,

§ 113a Speicherungspflichten für Daten

(1) Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ist verpflichtet, von ihm bei der Nutzung seines Dienstes erzeugte oder verarbeitete Verkehrsdaten nach Maßgabe der Absätze 2 bis 5 sechs Monate im Inland oder in einem anderen Mitgliedstaat der Europäischen Union zu speichern. Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ohne selbst Verkehrsdaten zu erzeugen oder zu verarbeiten, hat sicherzustellen, dass die Daten gemäß Satz 1 gespeichert werden, und der Bundesnetzagentur auf deren Verlangen mitzuteilen, wer diese Daten speichert.

(2) Die Anbieter von öffentlich zugänglichen Telefondiensten speichern: ...

(3) Die Anbieter von Diensten der elektronischen Post speichern: ...

(4) Die Anbieter von Internetzugangsdiensten speichern: ...

...

D.2 Auszug aus der deutschen Telekommunikations-Überwachungsverordnung (TKÜV)

Stand: Telekommunikations-Überwachungsverordnung vom 3. November 2005 (BGBl. I S. 3136), geändert durch Artikel 13 des Gesetzes vom 21. Dezember 2007 (BGBl. I S. 3198) [TKÜV 2005]

§ 3 Kreis der Verpflichteten

(1) Die Vorschriften dieses Teils gelten für die Betreiber von Telekommunikationsanlagen, mit denen Telekommunikationsdienste für die Öffentlichkeit erbracht werden. Werden mit einer Telekommunikationsanlage sowohl Telekommunikationsdienste für die Öffentlichkeit als auch andere Telekommunikationsdienste erbracht, gilt dies nur für den Teil der Telekommunikationsanlage, der der Erbringung von Telekommunikationsdiensten für die Öffentlichkeit dient.

(2) Für Telekommunikationsanlagen im Sinne von Absatz 1 müssen keine Vorkehrungen getroffen werden, soweit

1. es sich um ein Telekommunikationsnetz handelt, das Teilnehmernetze miteinander verbindet und keine Telekommunikationsanschlüsse aufweist,
2. sie Netzknoten sind, die der Zusammenschaltung mit dem Internet dienen,
3. sie aus Übertragungswegen gebildet werden, es sei denn, dass diese dem unmittelbaren teilnehmerbezogenen Zugang zum Internet dienen,
4. sie ausschließlich der Verteilung von Rundfunk oder anderen für die Öffentlichkeit bestimmten Diensten, dem Abruf von allgemein zugänglichen Informationen oder der Übermittlung von Messwerten, nicht individualisierten Daten, Notrufen oder Informationen für die Sicherheit und Leichtigkeit des See- oder Luftverkehrs dienen, oder
5. an sie nicht mehr als 10.000 Teilnehmer oder sonstige Nutzungsberechtigte angeschlossen sind.

Satz 1 Nr. 1 und 5 gilt nicht für Netzknoten, die der Vermittlung eines öffentlich zugänglichen Telefondienstes ins Ausland dienen. Satz 1 Nr. 1 und 2 gilt nicht im Hinblick auf Vorkehrungen zur Erfüllung der Verpflichtung aus § 110 Abs. 1 Satz 1 Nr. 1a des Telekommunikationsgesetzes. § 100b Abs. 3 Satz 1 der Strafprozessordnung, § 2 Abs. 1 Satz 3 des Artikel 10-Gesetzes, § 23a Abs. 8 des Zollfahndungsdienstgesetzes sowie die Vorschriften des Landesrechts über Maßnahmen zur Überwachung der Telekommunikation bleiben unberührt.

D.3 Auszug aus dem deutschen Telekommunikationsgesetz (TKG) alte Fassung

Stand: Telekommunikationsgesetz (TKG) vom 25. Juli 1996 (BGBl. I S. 1120), zuletzt geändert durch Gesetz vom 17.12.97 (BGBl. I 1997 S. 3108) [TKG aF]

§ 3 Begriffsbestimmungen

...

16 ist **"Telekommunikation"** der technische Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen,

17 sind **"Telekommunikationsanlagen"** technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische

Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können,

18 sind **"Telekommunikationsdienstleistungen"** das gewerbliche Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte,

...

D.4 Auszug aus der Europäischen Rahmenrichtlinie (RRL)

Stand: RICHTLINIE 2002/21/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie) [EU 2002/21/EG]

Artikel 2 Begriffsbestimmungen

a) "elektronisches Kommunikationsnetz": Übertragungssysteme und gegebenenfalls Vermittlungs- und Leitwegeinrichtungen sowie anderweitige Ressourcen, die die Übertragung von Signalen über Kabel, Funk, optische oder andere elektromagnetische Einrichtungen ermöglichen, einschließlich Satellitennetze, feste (leitungs- und paketvermittelte, einschließlich Internet) und mobile terrestrische Netze, Stromleitungssysteme, soweit sie zur Signalübertragung genutzt werden, Netze für Hör- und Fernsehfunk sowie Kabelfernsehnetze, unabhängig von der Art der übertragenen Informationen;

c) "elektronische Kommunikationsdienste": gewöhnlich gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen, jedoch ausgenommen Dienste, die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben; nicht dazu gehören die Dienste der Informationsgesellschaft im Sinne von Artikel 1 der Richtlinie 98/34/EG, die nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen;

d) "öffentliches Kommunikationsnetz": ein elektronisches Kommunikationsnetz, das ganz oder überwiegend zur Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste dient;

Artikel 8 Politische Ziele und regulatorische Grundsätze

(1) Die Mitgliedstaaten sorgen dafür, dass die nationalen Regulierungsbehörden bei der Wahrnehmung der in dieser Richtlinie und den Einzelrichtlinien festgelegten regulatorischen Aufgaben alle angezeigten Maßnahmen treffen, die den in den Absätzen 2, 3 und 4 vorgegebenen Zielen dienen. Die Maßnahmen müssen in angemessenem Verhältnis zu diesen Zielen stehen. Die Mitgliedstaaten sorgen dafür, dass die nationalen Regulierungsbehörden bei der Wahrnehmung der in dieser Richtlinie und den Einzelrichtlinien festgelegten regulatorischen Aufgaben, insbesondere der Aufgaben, die der Gewährleistung eines wirksamen Wettbewerbs dienen, weitestgehend berücksichtigen, dass die Regulierung technologieneutral sein sollte.

Die nationalen Regulierungsbehörden können im Rahmen ihrer Zuständigkeiten dazu beitragen, dass die Umsetzung von Maß- nahmen zur Förderung der kulturellen und sprachlichen Vielfalt sowie des Pluralismus der Medien sichergestellt werden.

Artikel 10 Vergabe von Nummern, Namen und Adressen

(5) Soweit es zur Sicherstellung der vollen globalen Interoperabilität der Dienste angebracht ist, koordinieren die Mitgliedstaaten ihre Standpunkte in internationalen Organisationen und Gremien, in denen Beschlüsse über Aspekte der Vergabe von Nummern, Namen und Adressen in elektronischen Kommunikationsnetzen und -diensten gefasst werden.

Artikel 25 Überprüfung

Die Kommission überprüft regelmäßig die Anwendung dieser Richtlinie und erstattet dem Europäischen Parlament und dem Rat darüber Bericht, und zwar erstmals spätestens drei Jahre nach dem Zeitpunkt des Beginns der Anwendung dieser Richtlinie gemäß Artikel 28 Absatz 1 Unterabsatz 2. Hierzu kann sie Informationen von den Mitgliedstaaten einholen, die ohne unangemessene Verzögerung zu liefern sind.

D.5 Auszug aus der Europäischen Zugangsrichtlinie

Stand: RICHTLINIE 2002/19/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 7. März 2002 über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung (Zugangsrichtlinie) [EU 2002/19/EG]

Artikel 5 Befugnisse und Zuständigkeiten der nationalen Regulierungsbehörden in Bezug auf Zugang und Zusammenschaltung

(1) Die nationalen Regulierungsbehörden fördern und garantieren gegebenenfalls entsprechend dieser Richtlinie bei ihren Maßnahmen zur Verwirklichung der in Artikel 8 der Richtlinie 2002/21/EG (Rahmenrichtlinie) festgelegten Ziele einen angemessenen Zugang und eine geeignete Zusammenschaltung sowie die Interoperabilität der Dienste und nehmen ihre Zuständigkeit in einer Weise wahr, die Effizienz fördert, den Wettbewerb stimuliert und den Endnutzern größtmöglichen Nutzen bringt. Unbeschadet etwaiger Maßnahmen gemäß Artikel 8 in Bezug auf Unternehmen mit beträchtlicher Marktmacht können die nationalen Regulierungsbehörden insbesondere folgende Maß- nahmen treffen:

a) In dem zur Gewährleistung des End-zu-End-Verbunds von Diensten erforderlichen Umfang können sie den Unternehmen, die den Zugang zu den Endnutzern kontrollieren, Verpflichtungen auferlegen, wozu in begründeten Fällen auch die Verpflichtung gehören kann, ihre Netze zusammenzuschalten, sofern dies noch nicht geschehen ist.

b) In dem zur Gewährleistung des Zugangs der Endnutzer zu vom Mitgliedstaat festgelegten digitalen Rundfunk- und Fernsehdiensten erforderlichen Umfang können sie die Betreiber dazu verpflichten, zu fairen, ausgewogenen und nichtdiskriminierenden Bedingungen den Zugang zu den in Anhang I Teil II aufgeführten anderen Einrichtungen zu gewähren.

D.6 Auszug aus dem österreichischen Telekommunikationsgesetz

Stand: Österreichisches Telekommunikationsgesetz 2003 (TKG 2003), Stammfassung: BGBl. I Nr. 70/2003, Bundesgesetz, idF BGBl I Nr. 133/2005 [TKG-Oe]

§ 3 Begriffsbestimmungen

9. "Kommunikationsdienst" eine gewerbliche Dienstleistung, die ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze besteht, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen, jedoch ausgenommen Dienste, die Inhalte über Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle

über sie ausüben. Ausgenommen davon sind Dienste der Informationsgesellschaft im Sinne von § 1 Abs. 1 Z 2 des Notifikationsgesetzes, BGBl. I Nr. 183/1999, die nicht ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze bestehen;

D.7 Auszug aus dem deutschen Teledienstegesetz (TDG)

Stand: Gesetz über die Nutzung von Telediensten (Teledienstegesetz - TDG) vom 22.07.1997 (BGBl. I S. 1870); zuletzt geändert durch Artikel 12 Abs. 15 G. vom 10.11.2006 BGBl. I S. 2553; aufgehoben durch Artikel 5 G. vom 26.02.2007 (BGBl. I S. 179) [TDG 97]

Hinweis: *nicht mehr in Kraft; abgelöst durch Telemediengesetz (TMG) [TMG 2007]*

§ 2 Geltungsbereich

(1) Die nachfolgenden Vorschriften gelten für alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt (Teledienste).

(2) Teledienste im Sinne des Absatzes 1 sind insbesondere

1. Angebote im Bereich der Individualkommunikation (zum Beispiel Telebanking, Datenaustausch),
2. Angebote zur Information oder Kommunikation, soweit nicht die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht (Datendienste, zum Beispiel Verkehrs-, Wetter-, Umwelt- und Börsendaten, Verbreitung von Informationen über Waren und Dienstleistungsangebote),
3. Angebote zur Nutzung des Internets oder weiterer Netze,
4. Angebote zur Nutzung von Telespielen,
5. Angebote von Waren und Dienstleistungen in elektronisch abrufbaren Datenbanken mit interaktivem Zugriff und unmittelbarer Bestellmöglichkeit.

(3) Absatz 1 gilt unabhängig davon, ob die Nutzung der Teledienste ganz oder teilweise unentgeltlich oder gegen Entgelt möglich ist.

(4) Dieses Gesetz gilt nicht für

1. Telekommunikationsdienstleistungen und das geschäftsmäßige Erbringen von Telekommunikationsdiensten nach § 3 des Telekommunikationsgesetzes vom 25. Juli 1996 (BGBl. I S. 1120),
2. Rundfunk im Sinne des § 2 des Rundfunkstaatsvertrages,
3. inhaltliche Angebote bei Verteildiensten und Abrufdiensten, soweit die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht, nach § 2 des Mediendienste-Staatsvertrages in der Fassung vom 20. Januar bis 7. Februar 1997,

§ 3 Begriffsbestimmungen Im Sinne dieses Gesetzes bezeichnet der Ausdruck

1. "Diensteanbieter" jede natürliche oder juristische Person, die eigene oder fremde Teledienste zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt;
2. "Nutzer" jede natürliche oder juristische Person, die zu beruflichen oder sonstigen Zwecken Teledienste in Anspruch nimmt, insbesondere um Informationen zu erlangen oder zugänglich zu machen;
3. "Verteildienste" Teledienste, die im Wege einer Übertragung von Daten ohne individuelle Anforderung gleichzeitig für eine unbegrenzte Zahl von Nutzern erbracht werden;
4. "Abrufdienste" Teledienste, die im Wege einer Übertragung von Daten auf Anforderung eines einzelnen Nutzers erbracht werden;

...

D.8 Auszug aus dem deutschen Telemediengesetz (TMG)

Stand: Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179) [TMG 2007]

§ 1 Anwendungsbereich

(1) Dieses Gesetz gilt für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind (Telemedien). Dieses Gesetz gilt für alle Anbieter einschließlich der öffentlichen Stellen unabhängig davon, ob für die Nutzung ein Entgelt erhoben wird.

(2) Dieses Gesetz gilt nicht für den Bereich der Besteuerung.

(3) Das Telekommunikationsgesetz und die Pressegesetze bleiben unberührt.

(4) Die an die Inhalte von Telemedien zu richtenden besonderen Anforderungen ergeben sich aus dem Staatsvertrag für Rundfunk und Telemedien (Rundfunkstaatsvertrag).

(5) Dieses Gesetz trifft weder Regelungen im Bereich des internationalen Privatrechts noch regelt es die Zuständigkeit der Gerichte.

§ 2 Begriffsbestimmungen Im Sinne dieses Gesetzes

1. ist Diensteanbieter jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt,

2. ist niedergelassener Diensteanbieter jeder Anbieter, der mittels einer festen Einrichtung auf unbestimmte Zeit Telemedien geschäftsmäßig anbietet oder erbringt; der Standort der technischen Einrichtung allein begründet keine Niederlassung des Anbieters,

3. ist Nutzer jede natürliche oder juristische Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen,

4. sind Verteildienste Telemedien, die im Wege einer Übertragung von Daten ohne individuelle Anforderung gleichzeitig für eine unbegrenzte Anzahl von Nutzern erbracht werden,

5. ist kommerzielle Kommunikation jede Form der Kommunikation, die der unmittelbaren oder mittelbaren Förderung des Absatzes von Waren, Dienstleistungen oder des Erscheinungsbilds eines Unternehmens, einer sonstigen Organisation oder einer natürlichen Person dient, die eine Tätigkeit im Handel, Gewerbe oder Handwerk oder einen freien Beruf ausübt; die Übermittlung der folgenden Angaben stellt als solche keine Form der kommerziellen Kommunikation dar:

   a) Angaben, die unmittelbaren Zugang zur Tätigkeit des Unternehmens oder der Organisation oder Person ermöglichen, wie insbesondere ein Domain-Name oder eine Adresse der elektronischen Post,

   b) Angaben in Bezug auf Waren und Dienstleistungen oder das Erscheinungsbild eines Unternehmens, einer Organisation oder Person, die unabhängig und insbesondere ohne finanzielle Gegenleistung gemacht werden.

Einer juristischen Person steht eine Personengesellschaft gleich, die mit der Fähigkeit ausgestattet ist, Rechte zu erwerben und Verbindlichkeiten einzugehen.

§ 4 Zulassungsfreiheit

Telemedien sind im Rahmen der Gesetze zulassungs- und anmeldefrei.

§ 5 Allgemeine Informationspflichten

(1) Diensteanbieter haben für geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten:

1. den Namen und die Anschrift, unter der sie niedergelassen sind, bei juristischen Personen zusätzlich die Rechtsform, den Vertretungsberechtigten und, sofern Angaben über das Kapital der Gesellschaft gemacht werden, das Stamm- oder Grundkapital sowie, wenn nicht alle in Geld zu leistenden Einlagen eingezahlt sind, der Gesamtbetrag der ausstehenden Einlagen,

2. Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit ihnen ermöglichen, einschließlich der Adresse der elektronischen Post,

3. soweit der Dienst im Rahmen einer Tätigkeit angeboten oder erbracht wird, die der behördlichen Zulassung bedarf, Angaben zur zuständigen Aufsichtsbehörde,

4. das Handelsregister, Vereinsregister, Partnerschaftsregister oder Genossenschaftsregister, in das sie eingetragen sind, und die entsprechende Registernummer,

5. soweit der Dienst in Ausübung eines Berufs im Sinne von Artikel 1 Buchstabe d der Richtlinie 89/48/EWG des Rates vom 21. Dezember 1988 über eine allgemeine Regelung zur Anerkennung der Hochschuldiplome, die eine mindestens dreijährige Berufsausbildung abschließen (ABl. EG Nr. L 19 S. 16), oder im Sinne von Artikel 1 Buchstabe f der Richtlinie 92/51/EWG des Rates vom 18. Juni 1992 über eine zweite allgemeine Regelung zur Anerkennung beruflicher Befähigungsnachweise in Ergänzung zur Richtlinie 89/48/EWG (ABl. EG Nr. L 209 S. 25, 1995 Nr. L 17 S. 20), zuletzt geändert durch die Richtlinie 97/38/EG der Kommission vom 20. Juni 1997 (ABl. EG Nr. L 184 S. 31), angeboten oder erbracht wird, Angaben über

a) die Kammer, welcher die Diensteanbieter angehören,

b) die gesetzliche Berufsbezeichnung und den Staat, in dem die Berufsbezeichnung verliehen worden ist,

c) die Bezeichnung der berufsrechtlichen Regelungen und dazu, wie diese zugänglich sind,

6. in Fällen, in denen sie eine Umsatzsteueridentifikationsnummer nach § 27a des Umsatzsteuergesetzes oder eine Wirtschafts-Identifikationsnummer nach § 139c der Abgabenordnung besitzen, die Angabe dieser Nummer,

7. bei Aktiengesellschaften, Kommanditgesellschaften auf Aktien und Gesellschaften mit beschränkter Haftung, die sich in Abwicklung oder Liquidation befinden, die Angabe hierüber.

(2) Weitergehende Informationspflichten nach anderen Rechtsvorschriften bleiben unberührt.

§ 9 Zwischenspeicherung zur beschleunigten Übermittlung von Informationen Diensteanbieter sind für eine automatische, zeitlich begrenzte Zwischenspeicherung, die allein dem Zweck dient, die Übermittlung fremder Informationen an andere Nutzer auf deren Anfrage effizienter zu gestalten, nicht verantwortlich, sofern sie

1. die Informationen nicht verändern,

2. die Bedingungen für den Zugang zu den Informationen beachten,

3. die Regeln für die Aktualisierung der Informationen, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, beachten,

4. die erlaubte Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Informationen, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, nicht beeinträchtigen und

5. unverzüglich handeln, um im Sinne dieser Vorschrift gespeicherte Informationen zu entfernen oder den Zugang zu ihnen zu sperren, sobald sie Kenntnis davon erhalten haben, dass die Informationen am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt wurden oder der Zugang zu ihnen gesperrt wurde oder ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperrung angeordnet hat.

§ 8 Abs. 1 Satz 2 gilt entsprechend.

D.9 Auszug aus dem Bundesdatenschutzgesetz (BDSG)

Stand: Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. August 2006 (BGBl. I S. 1970), neugefasst durch Bek. v. 14.1.2003 I 66; zuletzt geändert durch Art. 1 G v. 22.8.2006 I 1970 [BDSG 2003]

§ 1 Zweck und Anwendungsbereich des Gesetzes

(1) Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,

2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie

a) Bundesrecht ausführen oder

b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,

3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

...

§ 3a Datenvermeidung und Datensparsamkeit

Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Anlage (zu § 9 Satz 1) *Fundstelle des Originaltextes: BGBl. I 2003, 88*

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

D.10 Auszug aus dem Rundfunkstaatsvertrag (RStV)

Stand: Staatsvertrag für Rundfunk und Telemedien (Rundfunkstaatsvertrag - RStV) vom 31.08.1991, zuletzt geändert durch Artikel 1 des Neunten Staatsvertrages zur Änderung rundfunkrechtlicher Staatsverträge vom 31.07. bis 10.10.2006 (GBl. BW 2007 S. 111), in Kraft getreten am 01.03.2007 [RStV 2007]

§ 55 Informationspflichten und Informationsrechte

(1) Anbieter von Telemedien, die nicht ausschließlich persönlichen oder familiären Zwecken dienen, haben folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten:

1. Namen und Anschrift sowie

2. bei juristischen Personen auch Namen und Anschrift des Vertretungsberechtigten.

(2) Anbieter von Telemedien mit journalistisch-redaktionell gestalteten Angeboten, in denen insbesondere vollständig oder teilweise Inhalte periodischer Druckerzeugnisse in Text oder Bild wiedergegeben werden, haben zusätzlich zu den Angaben nach den §§ 5 und 6 des Telemediengesetzes einen Verantwortlichen mit Angabe des Namens und der Anschrift zu benennen. Werden mehrere Verantwortliche benannt, so ist kenntlich zu machen, für welchen Teil des Dienstes der jeweils Benannte verantwortlich ist. Als Verantwortlicher darf nur benannt werden, wer

1. seinen ständigen Aufenthalt im Inland hat,
2. nicht infolge Richterspruchs die Fähigkeit zur Bekleidung öffentlicher Ämter verloren hat,
3. voll geschäftsfähig ist und
4. unbeschränkt strafrechtlich verfolgt werden kann.

(3) Für Anbieter von Telemedien nach Absatz 2 Satz 1 gilt § 9a entsprechend.

Literaturverzeichnis

A-Drs. 16(9)530

Bizer, J.: *Stellungnahme zum Gesetzentwurf der Bundesregierung: Elektronisches-Geschäftsverkehr-Vereinheitlichungsgesetz (ElGVG), BT-Drs. 16/3078*, 2006

Aberer et al. 2005

Aberer, K. ; Alima, L. ; Ghodsi, A. ; Girdzijauskas, S. ; Haridi, S. ; Hauswirth, M.: The Essence of P2P: A Reference Architecture for Overlay Networks. In: *P2P '05: Proceedings of the Fifth IEEE International Conference on Peer-to-Peer Computing*, IEEE Computer Society, 2005. – DOI 10.1109/P2P.2005.38, S. 11–20

Aberer et al. 2003

Aberer, K. ; Cudre-Mauroux, P. ; Datta, A. ; Despotovic, Z. ; Hauswirth, M. ; Punceva, M. ; Schmidt, R.: P-Grid: a self-organizing structured P2P system. In: *SIGMOD Rec.* vol. 32, no. 3 (2003), S. 29–33. – DOI 10.1145/945721.945729. – ISSN 0163–5808

Aberer et al. 2002

Aberer, K. ; Punceva, M. ; Hauswirth, M. ; Schmidt, R.: Improving Data Access in P2P Systems. In: *IEEE Internet Computing* vol. 6, no. 1 (2002), S. 58–67. – DOI 10.1109/4236.978370. – ISSN 1089–7801

Agre 2003

Agre, P.: P2P and the promise of internet equality. In: *Commun. ACM* vol. 46, no. 2 (2003), S. 39–42. – DOI 10.1145/606272.606298. – ISSN 0001–0782

Alonso et al. 2004

Alonso, G. ; Casati, F. ; Kuno, H. ; Machiraju, V.: *Web Services: Concepts, Architecture and Applications*. Springer, 2004. – ISBN 3–540–44008–9

Anderson 1996

Anderson, R.: The Eternity Service. In: *Pragocrypt '96*, 1996, S. 242–252

Androutsellis-Theotokis & Spinellis 2004

Androutsellis-Theotokis, S. ; Spinellis, D.: A survey of peer-to-peer content distribution technologies. In: *ACM Comput. Surv.* vol. 36, no. 4 (2004), S. 335–371. – DOI 10.1145/1041680.1041681. – ISSN 0360–0300

Arak 2007

Arak, V.: *What happened on August 16*. (WWW-Veröffentlichung). 2007 `http://heartbeat.skype.com/2007/08/`

Awerbuch & Scheideler 2006

Awerbuch, B. ; Scheideler, C.: Towards a scalable and robust DHT. In: *SPAA '06: Proceedings of the eighteenth annual ACM symposium on Parallelism in algorithms and architectures*, ACM, 2006. – DOI 10.1145/1148109.1148163. – ISBN 1–59593–452–9, S. 318–327

Aweya 2001

Aweya, J.: IP router architectures: an overview. In: *International Journal of Communication Systems* vol. 14, no. 5 (2001), S. 447–475. – DOI 10.1002/dac.505

Balakrishnan et al. 2003

Balakrishnan, H. ; Kaashoek, M. ; Karger, D. ; Morris, R. ; Stoica, I.: Looking up data in P2P systems. In: *Commun. ACM* vol. 46, no. 2 (2003), S. 43–48. – DOI 10.1145/606272.606299. – ISSN 0001–0782

Balakrishnan et al. 2004

Balakrishnan, H. ; Lakshminarayanan, K. ; Ratnasamy, S. ; Shenker, S. ; Stoica, I. ; Walfish, M.: A layered naming architecture for the internet. In: *SIGCOMM '04: Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications*, ACM, 2004. – DOI 10.1145/1015467.1015505. – ISBN 1–58113–862–8, S. 343–352

Barborak et al. 1993

Barborak, M. ; Dahbura, A. ; Malek, M.: The consensus problem in fault-tolerant computing. In: *ACM Comput. Surv.* vol. 25, no. 2 (1993), S. 171–220. – DOI 10.1145/152610.152612. – ISSN 0360–0300

Barkai 2001

Barkai, D.: *Peer-to-Peer Computing: Technologies for Sharing and Collaborating on the Net*. Intel Press, 2001. – ISBN 0970284675

Baset & Schulzrinne 2006

Baset, S. ; Schulzrinne, H.: An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol. In: *INFOCOM 2006: Proceedings of the 25th IEEE International Conference on Computer Communications*, IEEE, 2006. – DOI 10.1109/INFOCOM.2006.312. – ISSN 0743–166X, S. 2695–2706

Bazzi & Konjevod 2005

Bazzi, R. ; Konjevod, G.: On the establishment of distinct identities in overlay networks. In: *PODC '05: Proceedings of the twenty-fourth annual ACM symposium on Principles of distributed computing*, ACM, 2005. – DOI 10.1145/1073814.1073873. – ISBN 1–59593–994–2, S. 312–320

BDSG 2003

Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. August 2006 (BGBl. I S. 1970) `http://www.gesetze-im-internet.de/bdsg_1990/`

Bernstein 1996

Bernstein, P.: Middleware: a model for distributed system services. In: *Commun. ACM* vol. 39, no. 2 (1996), S. 86–98. – DOI 10.1145/230798.230809. – ISSN 0001–0782

Biondi & Desclaux

Biondi, P. ; Desclaux, F.: *Silver Needle in the Skype*. Black Hat Europe 2006 (WWW-Veröffentlichung), 2006.
`http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-biondi/bh-eu-06-biondi-up.pdf`

BitT BEP3 2008

Loewenstern, A.: *BitTorrent Protocol Specification: BEP 3: The BitTorrent Protocol Specification (Final, V. 11031)*. (WWW-Veröffentlichung). 2008
`http://www.bittorrent.org/beps/bep_0003.html`

BitT BEP5 2008

Loewenstern, A.: *BitTorrent Protocol Specification: BEP 5: DHT Protocol (Draft, V. 11031)*. (WWW-Veröffentlichung). 2008
`http://www.bittorrent.org/beps/bep_0005.html`

Blumenthal & Clark 2001

Blumenthal, M. ; Clark, D.: Rethinking the design of the Internet: the end-to-end arguments vs. the brave new world. In: *ACM Trans. Interet Technol.* vol. 1, no. 1 (2001), S. 70–109. – DOI 10.1145/383034.383037. – ISSN 1533–5399

BNetzA 2005

Eckpunkte der regulatorischen Behandlung von Voice over IP (VoIP) vom 09.09.2005. Bundesnetzagentur (BNetzA), (WWW-Veröffentlichung). 2005
`http://www.bundesnetzagentur.de/media/archive/3210.pdf`

BNetzA 2006

Frageweise Auswertung der Anhörung zu Voice over IP (VoIP). Bundesnetzagentur, (WWW-Veröffentlichung). 2006
`http://www.bundesnetzagentur.de/media/archive/3171.pdf`

Borisov 2006

Borisov, N.: Computational Puzzles as Sybil Defenses. In: *P2P '06: Proceedings of the Sixth IEEE International Conference on Peer-to-Peer Computing*, IEEE Computer Society, 2006. – DOI 10.1109/P2P.2006.10. – ISBN 0–7695–2679–9, S. 171–176

BR-Drs. 359/06

BR-Drs. 359/06, Stellungnahme des Bundesrates, Entwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Vorschriften, 2006

BR-Drs. 556/06

Entwurf eines Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz - ElGVG) vom 11.08.2006, 2006

Bracha & Toueg 1985

Bracha, G. ; Toueg, S.: Asynchronous consensus and broadcast protocols. In: *Journal of the ACM* vol. 32, no. 4 (1985), S. 824–840. – DOI 10.1145/4221.214134. – ISSN 0004–5411

Bramhall et al. 2007

Bramhall, P. ; Hansen, M. ; Rannenberg, K. ; Roessler, T.: User-Centric Identity Management: New Trends in Standardization and Regulation. In: *IEEE Security and Privacy* vol. 5, no. 4 (2007), S. 84–87. – DOI 10.1109/MSP.2007.99. – ISSN 1540–7993

Bronstein et al. 1997

Bronstein, I. ; Semendjajew, K. ; Musiol, G.: *Taschenbuch der Mathematik*. Deutsch Harri GmbH, Auflage: 3., überarb. u. erw. A., 1997. – ISBN 3–8171–2003–6

Brunst 2004

Brunst, P.: Umsetzungsprobleme der Impressumspflicht bei Webangeboten. In: *Multimedia und Recht (MMR), Heft 1/2004* (2004), S. 8–13. – ISSN 1434–596X

BT-Drs. 14/6098

BT-Drs. 14/6098, Entwurf eines Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz – EGG), 2001. `http://dip.bundestag.de/btd/14/060/1406098.pdf`

BT-Drs. 15/2316

BT-Drs. 15/2316, Entwurf eines Telekommunikationsgesetzes (TKG), 2004. `http://dip.bundestag.de/btd/15/023/1502316.pdf`

BT-Drs. 16/2581

BT-Drs. 16/2581, Entwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Vorschriften, 2006. http://dip.bundestag.de/btd/16/025/1602581.pdf

BT-Drs. 16/3635

BT-Drs. 16/3635, Beschlussempfehlung und Bericht des Ausschusses für Wirtschaft und Technologie (9. Ausschuss), 2006. http://dip.bundestag.de/btd/16/036/1603635.pdf

Buragohain et al. 2003

Buragohain, C. ; Agrawal, D. ; Suri, S.: A Game Theoretic Framework for Incentives in P2P Systems. In: *P2P '03: Proceedings of the 3rd International Conference on Peer-to-Peer Computing*, IEEE Computer Society, 2003. – ISBN 0–7695–2023–5, S. 48–56

BVerfG 1 BvR 370/07

Bundesverfassungsgericht: *Leitsätze zum Urteil des Ersten Senats vom 27. Februar 2008 (1 BvR 370/07, 1 BvR 595/07), BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1-333)*, 2008. http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html

Carzaniga & Wolf 2002

Carzaniga, A. ; Wolf, A.: Content-Based Networking: A New Communication Infrastructure. In: *IMWS '01: Revised Papers from the NSF Workshop on Developing an Infrastructure for Mobile and Wireless Systems*, Springer-Verlag, 2002. – DOI 10.1007/3–540–36257–6. – ISBN 3–540–00289–8, S. 59–68

Castro et al. 2005

Castro, M. ; Costa, M. ; Rowstron, A.: Debunking some myths about structured and unstructured overlays. In: *NSDI'05: Proceedings of the 2nd Symposium on Networked Systems Design and Implementation*, USENIX Association, 2005, S. 85–98

Castro et al. 2002a

Castro, M. ; Druschel, P. ; Ganesh, A. ; Rowstron, A. ; Wallach, D.: Secure routing for structured peer-to-peer overlay networks. In: *SIGOPS Oper. Syst. Rev.* vol. 36, no. SI (2002), S. 299–314. – DOI 10.1145/844128.844156. – ISSN 0163–5980

Castro et al. 2002b

Castro, M. ; Druschel, P. ; Kermarrec, A.-M. ; Rowstron, A.: One ring to rule them all: service discovery and binding in structured peer-to-peer overlay networks. In: *EW10: Proceedings of the 10th workshop on ACM SIGOPS European workshop*, ACM, 2002. – DOI 10.1145/1133373.1133399, S. 140–145

Castro & Liskov 2002

Castro, M. ; Liskov, B.: Practical byzantine fault tolerance and proactive recovery. In: *ACM Trans. Comput. Syst.* vol. 20, no. 4 (2002), S. 398–461. – DOI 10.1145/571637.571640. – ISSN 0734–2071

Chaum 1981

Chaum, D.: Untraceable electronic mail, return addresses, and digital pseudonyms. In: *Commun. ACM* vol. 24, no. 2 (1981), S. 84–90. – DOI 10.1145/358549.358563. – ISSN 0001–0782

Chawathe et al. 2003

Chawathe, Y. ; Ratnasamy, S. ; Breslau, L. ; Lanham, N. ; Shenker, S.: Making gnutella-like P2P systems scalable. In: *SIGCOMM '03: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, ACM, 2003. – DOI 10.1145/863955.864000. – ISBN 1–58113–735–4, S. 407–418

Cheng & Friedman 2005

Cheng, A. ; Friedman, E.: Sybilproof reputation mechanisms. In: *P2PECON '05: Proceedings of the 2005 ACM SIGCOMM workshop on Economics of peer-to-peer systems*, ACM, 2005. – DOI 10.1145/1080192.1080202. – ISBN 1–59593–026–4, S. 128–132

Chu et al. 2001

Chu, Y. ; Rao, S. ; Seshan, S. ; Zhang, H.: Enabling conferencing applications on the internet using an overlay muilticast architecture. In: *SIGCOMM Comput. Commun. Rev.* vol. 31, no. 4 (2001), S. 55–67. – DOI 10.1145/964723.383064. – ISSN 0146–4833

Clark 1988

Clark, D.: The design philosophy of the DARPA internet protocols. In: *SIGCOMM '88: Symposium proceedings on Communications architectures and protocols*, ACM, 1988. – DOI 10.1145/52324.52336. – ISBN 0–89791–279–9, S. 106–114

Clark 2005

Clark, D.: *What is Architecture? (V4.0).* (WWW-Veröffentlichung). 2005 `http://find.isi.edu/presentation_files/Dave_Clark-What_is_architecture_4.pdf`

Clark et al. 2005

Clark, D. ; Partridge, C. ; Braden, R. ; Davie, B. ; Floyd, S. ; Jacobson, V. ; Katabi, D. ; Minshall, G. ; Ramakrishnan, K. ; Roscoe, T. ; Stoica, I. ; Wroclawski, J. ; Zhang, L.: Making the world (of communications) a different place. In: *SIGCOMM Comput. Commun. Rev.* vol. 35, no. 3 (2005), S. 91–96. – DOI 10.1145/1070873.1070887. – ISSN 0146–4833

Clarke et al. 2001

Clarke, I. ; Sandberg, O. ; Wiley, B. ; Hong, T.: Freenet: a distributed anonymous information storage and retrieval system. In: *International workshop on Designing privacy enhancing technologies*, Springer, 2001. – DOI 10.1007/3–540–44702–4. – ISBN 3–540–41724–9, S. 46–66

Cohen 2003

Cohen, B.: Incentives build robustness in BitTorrent. In: *In Proceedings of the 1st Workshop on Economics of Peer-to-Peer Systems (P2PECON)*, 2003

Cohen & Shenker 2002

Cohen, E. ; Shenker, S.: Replication strategies in unstructured peer-to-peer networks. In: *SIGCOMM '02: Proceedings of the 2002 conference on Applications, technologies, architectures, and protocols for computer communications*, ACM, 2002. – DOI 10.1145/633025.633043. – ISBN 1–58113–570–X, S. 177–190

Conrad et al. 2005a

Conrad, M. ; Dinger, J. ; Hartenstein, H. ; Rolli, D. ; Schöller, M. ; Zitterbart, M.: A Peer-to-Peer Framework for Electronic Markets. 2005. In: Steinmetz, R. (Hrsg.) ; Wehrle, K. (Hrsg.): *Peer-to-Peer Systems and Applications (LNCS 3485)*. Springer, 2005. – DOI 10.1007/11530657. – ISBN 3–540–29192–X, S. 509–525

Conrad et al. 2005b

Conrad, M. ; Dinger, J. ; Hartenstein, H. ; Schöller, M. ; Zitterbart, M.: Combining Service-Orientation and Peer-to-Peer Networks. In: *Kommunikation in Verteilten Systemen (KiVS), Kurzbeiträge und Workshop der 14. GI/ITG-Fachtagung Kommunikation in Verteilten Systemen (KiVS 2005) Kaiserslautern, 28. Februar - 3. März 2005 (LNI 61)*, GI, 2005. – ISBN 3–88579–390–3, S. 181–184

Conrad & Hof 2007

Conrad, M. ; Hof, H.-J.: A Generic, Self-Organizing, and Distributed Bootstrap Service for Peer-to-Peer Networks. In: *Self-Organizing Systems: Second International Workshop, IWSOS 2007, Proceedings (LNCS 4725)*, Springer, 2007. – DOI 10.1007/978–3–540–74917–2. – ISBN 978–3–540–74916–5, S. 59–72

Coulouris et al. 2005

Coulouris, G. ; Dollimore, J. ; Kindberg, T.: *Distributed systems : concepts and design*. 4th edition. Addison-Wesley, 2005. – ISBN 0–321–26354–5

Cramer et al. 2004

Cramer, C. ; Kutzner, K. ; Fuhrmann, T.: Bootstrapping locality-aware P2P networks. In: *Networks, 2004. (ICON 2004). Proceedings. 12th IEEE International Conference on*, 2004. – DOI 10.1109/ICON.2004.1409169. – ISSN 1531–2216, S. 357–361

Crosby & Wallach 2007

Crosby, S. ; Wallach, D.: An Analysis of BitTorrent's Two Kademlia-Based DHTs. 2007. http://www.cs.rice.edu/~scrosby/tr/BTMeasure-Main.pdf. Department of Computer Science, Rice University, 2007 (TR-07-04). – Forschungsbericht

Crowcroft & Pratt 2002

Crowcroft, J. ; Pratt, I.: Peer to Peer: Peering into the Future. In: *Advanced Lectures on Networking : NETWORKING 2002 Tutorials (LNCS 2497)*, Springer, 2002. – DOI 10.1007/3–540–36162–6. – ISSN 1611–3349, S. 1–19

Dabek et al. 2003

Dabek, F. ; Zhao, B. ; Druschel, P. ; Kubiatowicz, J. ; Stoica, I.: Towards a Common API for Structured Peer-to-Peer Overlays. In: *Peer-to-Peer Systems II : Second International Workshop, IPTPS 2003 Berkeley, CA, USA, February 21-22, 2003 Revised Papers (LNCS 2735)*, Springer, 2003. – DOI 10.1007/b11823. – ISBN 978–3–540–40724–9, S. 33–44

Danezis et al. 2005

Danezis, G. ; Lesniewski-Laas, C. ; Kaashoek, F. ; Anderson, R.: Sybil-Resistant DHT Routing. In: *Computer Security – ESORICS 2005: 10th European Symposium on Research in Computer Security, Proceedings (LNCS 3679)*, Springer, 2005. – DOI 10.1007/11555827. – ISBN 978–3–540–28963–0, S. 305–318

de Meer & Koppen 2005

de Meer, H. ; Koppen, C.: Characterization of Self-Organization. 2005. In: Steinmetz, R. (Hrsg.) ; Wehrle, K. (Hrsg.): *Peer-to-Peer Systems and Applications (LNCS 3485)*. Springer, 2005. – DOI 10.1007/11530657. – ISBN 3–540–29192–X, S. 227–246

Deering 1998

Deering, S.: *Watching the Waist of the Protocol Hourglass*. Keynote address at the 6th IEEE International Conference on Network Protocols (ICNP). 1998 http://www.ieee-icnp.org/1998/Keynote.ppt

Dhungel et al. 2008

Dhungel, P. ; Wu, D. ; Schonhorst, B. ; Ross, K.: *A Measurement Study of Attacks on BitTorrent Leechers*. 7th International Workshop on Peer-to-Peer Systems, IPTPS 2008 (WWW-Veröffentlichung). 2008 http://www.cs.toronto.edu/iptps2008/final/47.pdf

Dinger & Hartenstein 2005

Dinger, J. ; Hartenstein, H.: On the challenge of assessing overlay topology adaptation mechanisms. In: *Peer-to-Peer Computing, 2005. P2P 2005. Fifth IEEE*

International Conference on, IEEE Computer Society, 2005. – DOI 10.1109/P2P.2005.22. – ISBN 0–7695–2376–5, S. 145–147

Dinger & Hartenstein 2006a
Dinger, J. ; Hartenstein, H.: Defending the Sybil Attack in P2P Networks: Taxonomy, Challenges, and a Proposal for Self-Registration. In: *Proceedings of the First International Conference on Availability, Reliability and Security (ARES 2006)*, IEEE Computer Society, 2006. – DOI 10.1109/ARES.2006.45. – ISBN 0–7695–2567–9, S. 756–763

Dinger & Hartenstein 2006b
Dinger, J. ; Hartenstein, H.: Die vermeintliche Robustheit von Peer-to-Peer-Netzen. In: *20. DFN-Jahrestagung (DFN2006) 06.06.2006 - 09.06.2006 Heilbronn, Deutschland,* `http://nbn-resolving.de/urn:nbn:de:kobv:11-10076045`, 2006, S. 182–192

Dinger & Hartenstein 2008
Dinger, J. ; Hartenstein, H.: *Netzwerk- und IT-Sicherheitsmanagement : Eine Einführung*. Universitätsverlag Karlsruhe, 2008. – ISBN 978–3–86644–209–2

Dinger et al. 2008
Dinger, J. ; Jünemann, K. ; Waldhorst, O. ; Conrad, M.: Autonome Kommunikationsinfrastrukturen: Eine praxisnahe Betrachtung. In: *PIK - Praxis der Informationsverarbeitung und Kommunikation* Jg. 31, Nr. 2 (2008), S. 69–75. – DOI 10.1515/piko.2008.0015. – ISSN 1066–8888

Dinger et al. 2006
Dinger, J. ; Raabe, O. ; Hartenstein, H.: A Techno-Legal Perspective on Peer-to-Peer-Based Bandwidth on Demand Management. In: *Bandwidth on Demand, 2006 1st IEEE International Workshop on*, IEEE Computer Society, 2006. – DOI 10.1109/BOD.2006.320802. – ISBN 1–4244–0793–1, S. 73–80

Dingledine et al. 2004
Dingledine, R. ; Mathewson, N. ; Syverson, P.: Tor: the second-generation onion router. In: *SSYM'04: Proceedings of the 13th conference on USENIX Security Symposium*, USENIX Association, 2004

Donath 1998
Donath, J.: Identity and Deception in the Virtual Community. In: Smith, M. (Hrsg.) ; Kollock, P. (Hrsg.): *Communities in Cyberspace*. Routledge, 1998. – ISBN 978–0415191401, S. 29–59

Douceur 2002

Douceur, J.: The Sybil Attack. In: *Peer-to-Peer Systems: 1st International Workshop on Peer-to-Peer Systems (IPTPS 2002), Revised Papers (LNCS 2429)*, Springer, 2002. – DOI 10.1007/3–540–45748–8. – ISBN 978–3–540–44179–3, S. 251–260

Eberspächer & Schollmeier 2005
Eberspächer, J. ; Schollmeier, R.: First and Second Generation of Peer-to-Peer Systems. 2005. In: Steinmetz, R. (Hrsg.) ; Wehrle, K. (Hrsg.): *Peer-to-Peer Systems and Applications (LNCS 3485)*. Springer, 2005. – DOI 10.1007/11530657. – ISBN 3–540–29192–X, S. 35–56

Eplus Agb
E-Plus Service GmbH & Co. KG: *Besondere Bedingungen, Leistungsbeschreibung und Preisliste für Mobilfunkdienstleistungen der BASE Handy- und Internetflatrate, gültig ab 10. 5. 2006, Teil C, Nr. 5*, 2006. http://www.base.de/downloads/BASE_besondere_Bedingungen_Handy_Internet.pdf

EU 2006a
Commission of the European Communities: *Commission Staff Working Document from the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, on the Review of the EU Regulatory Framework for electronic communications networks and services (SEC (2006) 816), 28.06.2006*. 2006 http://ec.europa.eu/information_society/policy/ecomm/doc/info_centre/public_consult/review/staffworkingdocument_final.pdf,http://ec.europa.eu/information_society/policy/ecomm/info_centre/documentation/public_consult/review_2/index_en.htm

EU 2006b
Stellungnahme der Bundesregierung der Bundesrepublik Deutschland zur Mitteilung der Kommission an den Rat, das Europäische Parlament, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über die Überprüfung des EU-Rechtsrahmens für elektronische Kommunikationsnetze und -dienste. 2006 http://ec.europa.eu/information_society/policy/ecomm/doc/info_centre/public_consult/review_2/comments/stn_de_endg_261006.pdf

EU 2000/31/EG
Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr" - "e-commerce Richtlinie"). Amtsblatt der Europäischen Gemeinschaften (ABl.) L 178 vom 17.07.2000 S. 1 ff., , 2000

EU 2001/C 96/02

Bekanntmachung der Kommission über einen Richtlinienentwurf über den Wettbewerb auf dem Markt für elektronische Kommunikationsdienste (2001/C 96/02). Amtsblatt der Europäischen Gemeinschaften (ABl.) vom 27.3.2001, C 96/02, 2001. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2001:096:0002:0007:DE:PDF

EU 2002/19/EG

Richtlinie 2002/19/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung (ZugangsRichtlinie). Amtsblatt der Europäischen Gemeinschaften (ABl.) Nr. L 108 vom 24.4.2002, S. 7 ff., 2002. http://ec.europa.eu/information_society/policy/ecomm/library/legislation/index_en.htm

EU 2002/20/EG

Richtlinie 2002/20/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über die Genehmigung elektronischer Kommunikationsnetze und -dienste (GenehmigungsRichtlinie). Amtsblatt der Europäischen Gemeinschaften (ABl.) Nr. L 108 vom 24.4.2002, S. 21 ff., 2002. http://ec.europa.eu/information_society/policy/ecomm/library/legislation/index_en.htm

EU 2002/21/EG

Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (RahmenRichtlinie, RRL). Amtsblatt der Europäischen Gemeinschaften (ABl.) Nr. L 108 vom 24.4.2002, S. 33 ff., 2002. http://ec.europa.eu/information_society/policy/ecomm/library/legislation/index_en.htm

EU 2002/22/EG

Richtlinie 2002/22/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten (UniversaldienstRichtlinie). Amtsblatt der Europäischen Gemeinschaften (ABl.) Nr. L 108 vom 24.4.2002, S. 51 ff., 2002. http://ec.europa.eu/information_society/policy/ecomm/library/legislation/index_en.htm

EU 2002/58/EG

Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (DatenschutzRichtlinie für elektronische Kommunikation). Amtsblatt der Europäischen Gemeinschaften (ABl.) Nr. L 108

vom 24.4.2002, S. 37 ff., 2002. http://ec.europa.eu/information_society/policy/ecomm/library/legislation/index_en.htm

EU 95/46/EG

Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Amtsblatt der Europäischen Gemeinschaften (ABl.) Nr. L 281 vom 23/11/1995 S. 31 ff., , 1995

EU 98/34/EG

Richtlinie 98/34/EG des Europäischen Parlaments und des Rates über Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft. Amtsblatt der Europäischen Gemeinschaften (ABl.) Nr. L 204 S. 37 ff., , 1998

EU Kons 2008

Kommission, Europäische: *Einführung in die öffentliche Konsultation zur RFID Empfehlung zur Privatsphäre, zum Datenschutz und zur Sicherheit*. (WWW-Veröffentlichung), 2008. http://ec.europa.eu/information_society/policy/rfid/doc/consde.pdf

EU Prj Prime

Fischer-Hübner, S. ; (eds.), H. H.: *PRIME Framework Version 3 (17 March, 2008)*, 2008. https://www.prime-project.eu/prime_products/reports/fmwk/pub_del_D14.1.c_ec_wp14.1_v1_final.pdf

Fairley 1990

Fairley, J.: Open network management. In: *Network Management and Signalling, IEE Colloquium on* (1990), S. 10/1–10/3

Falkner et al. 2007

Falkner, J. ; Piatek, M. ; John, J. ; Krishnamurthy, A. ; Anderson, T.: Profiling a Million User DHT. In: *IMC '07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, ACM, 2007. – DOI 10.1145/1298306.1298325. – ISBN 978–1–59593–908–1, S. 129–134

Fattah 2002

Fattah, H.: *P2P: How Peer-to-Peer Technology Is Revolutionizing the Way We Do Business*. Dearborn Trade Publishing, 2002. – ISBN 0–7931–4878–2

Feldman et al. 2004

Feldman, M. ; Lai, K. ; Stoica, I. ; Chuang, J.: Robust incentive techniques for peer-to-peer networks. In: *EC '04: Proceedings of the 5th ACM conference on Electronic commerce*, ACM, 2004. – DOI 10.1145/988772.988788. – ISBN 1–58113–711–0, S. 102–111

Feldman et al. 2006

Feldman, M. ; Papadimitriou, C. ; Chuang, J. ; Stoica, I.: Free-riding and whitewashing in peer-to-peer systems. In: *Selected Areas in Communications, IEEE Journal on* vol. 24, no. 5 (2006), May, S. 1010–1019. – DOI 10.1109/JSAC.2006.872882. – ISSN 0733–8716

Fiat et al. 2005

Fiat, A. ; Saia, J. ; Young, M.: Making Chord Robust to Byzantine Attacks. In: *Algorithms – ESA 2005: 13th Annual European Symposium, Proceedings (LNCS 3669)*, Springer, 2005. – DOI 10.1007/11561071. – ISBN 978–3–540–29118–3, S. 803–814

FIP 180-1

National Institute of Standards and Technology (NIST): *Secure Hash Standard*. Federal Information Processing Standards Publication 180-1, 1995. `http://www.itl.nist.gov/fipspubs/fip180-1.htm`

FIP 180-2

National Institute of Standards and Technology (NIST): *Secure Hash Standard*. Federal Information Processing Standards Publication 180-2, 2002. `http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf`

Fischer et al. 1985

Fischer, M. ; Lynch, N. ; Paterson, M.: Impossibility of distributed consensus with one faulty process. In: *J. ACM* vol. 32, no. 2 (1985), S. 374–382. – DOI 10.1145/3149.214121. – ISSN 0004–5411

Forster & De Meer 2004

Forster, F. ; De Meer, H.: Discovery of Web Services with a P2P Network. In: *Computational Science - ICCS 2004 (LNCS 3038), Workshop on First International Workshop on Active and Programmable Grids Architectures and Components*, Springer-Verlag, 2004. – DOI 10.1007/b97989. – ISBN 978–3–540–22116–6, S. 90–97

Foster 2002

Foster, I.: What is the Grid? A Three Point Checklist. In: *Daily News and Information for the Global Grid Community* vol. 1, no. 6 (2002). `http://www.gridtoday.com/02/0722/100136.html`

Foster & Iamnitchi 2003

Foster, I. ; Iamnitchi, A.: On Death, Taxes, and the Convergence of Peer-to-Peer and Grid Computing. In: *Peer-to-Peer Systems II : Second International Workshop, IPTPS 2003 Berkeley, CA, USA, February 21-22, 2003 Revised Papers (LNCS 2735)*, Springer, 2003. – DOI 10.1007/b11823. – ISBN 978–3–540–40724–9, S. 118–128

Foster & Kesselman 1999

Foster, I. (Hrsg.) ; Kesselman, C. (Hrsg.): *The Grid: Blueprint for a New Computing Infrastructure*. Morgan Kaufmann Publishers Inc., 1999. – ISBN 1–55860–475–8

Foster et al. 2001

Foster, I. ; Kesselman, C. ; Tuecke, S.: The Anatomy of the Grid: Enabling Scalable Virtual Organizations. In: *Int. J. High Perform. Comput. Appl.* vol. 15, no. 3 (2001), S. 200–222. – DOI 10.1177/109434200101500302. – ISSN 1094–3420

Freedman et al. 2004

Freedman, M. ; Freudenthal, E. ; Mazières, D.: Democratizing content publication with coral. In: *NSDI'04: Proceedings of the 1st conference on Symposium on Networked Systems Design and Implementation*, USENIX Association, 2004

Freedman & Morris 2002

Freedman, M. ; Morris, R.: Tarzan: a peer-to-peer anonymizing network layer. In: *CCS '02: Proceedings of the 9th ACM conference on Computer and communications security*, ACM, 2002. – DOI 10.1145/586110.586137. – ISBN 1–58113–612–9, S. 193–206

Galatopoullos et al. 2008

Galatopoullos, D. ; Kalofonos, D. ; Manolakos, E.: A P2P SOA enabling group collaboration through service composition. In: *ICPS '08: Proceedings of the 5th international conference on Pervasive services*, ACM, 2008. – DOI 10.1145/1387269.1387289. – ISBN 978–1–60558–135–4, S. 111–120

Gamma et al. 2004

Gamma, E. ; Helm, R. ; Johnson, R. ; Vlissides, J.: *Entwurfsmuster: Elemente wiederverwendbarer objektorientierter Software*. Addison-Wesley, 2004. – ISBN 3–8273–2199–9. – Übersetzung: D. Riehle

Gerke & Hausheer 2005

Gerke, J. ; Hausheer, D.: Peer-to-Peer Market Management. 2005. In: Steinmetz, R. (Hrsg.) ; Wehrle, K. (Hrsg.): *Peer-to-Peer Systems and Applications (LNCS 3485)*. Springer, 2005. – DOI 10.1007/11530657. – ISBN 3–540–29192–X, S. 491–507

Gerke & Stiller 2005

Gerke, J. ; Stiller, B.: A Service-Oriented Peer-to-Peer Middleware. In: *Kommunikation in Verteilten Systemen (KiVS)*, Springer-Verlag, 2005. – DOI 10.1007/b138861, S. 3–15

Gnutella WebCache

Website of the Gnutella Web Caching System (GWebCache), 2008. `http://www.gnucleus.com/gwebcache/`

Gong 2001

Gong, L.: JXTA: A Network Programming Environment. In: *IEEE Internet Computing* 5 (2001), Nr. 3, S. 88–95. – DOI 10.1109/4236.935182. – ISSN 1089–7801

Granville et al. 2005

Granville, L. ; Rosa, D. da ; Panisson, A. ; Melchiors, C. ; Almeida, M. ; Tarouco, L.: Managing computer networks using peer-to-peer technologies. In: *Communications Magazine, IEEE* vol. 43, no. 10 (2005), S. 62–68. – DOI 10.1109/MCOM.2005.1522126. – ISSN 0163–6804

Götz et al. 2005

Götz, S. ; Rieche, S. ; Wehrle, K.: Selected DHT Algorithms. 2005. In: Steinmetz, R. (Hrsg.) ; Wehrle, K. (Hrsg.): *Peer-to-Peer Systems and Applications (LNCS 3485)*. Springer, 2005. – DOI 10.1007/11530657. – ISBN 3–540–29192–X, S. 95–117

Guttman 1999

Guttman, E.: Service Location Protocol: Automatic Discovery of IP Network Services. In: *IEEE Internet Computing* vol. 3, no. 4 (1999), S. 71–80. – DOI 10.1109/4236.780963. – ISSN 1089–7801

Haßlinger 2005

Hasslinger, G.: ISP Platforms Under a Heavy Peer-to-Peer Workload. 2005. In: Steinmetz, R. (Hrsg.) ; Wehrle, K. (Hrsg.): *Peer-to-Peer Systems and Applications (LNCS 3485)*. Springer, 2005. – DOI 10.1007/11530657. – ISBN 3–540–29192–X, S. 369–381

Halsall 2005

Halsall, F.: *Computer Networking and the Internet*. 5th edition. Addison Wesley, 2005. – ISBN 0–321–26358–8

Hansen et al. 2007

Hansen, M. ; Pfitzmann, A. ; Rossnagel, A.: Online-Durchsuchung. In: *Deutsche Richterzeitung (DRiZ), Heft 8/2007* (2007), S. 225–230. – ISSN 0340–8612

Hausheer 2006

Hausheer, D.: *PeerMart: Secure Decentralized Pricing and Accounting for Peer-to-Peer Systems (Diss. ETH Zurich No. 16200)*. Shaker Verlag, 2006. – ISBN 3–8322–4969–9

Hellerstein 2003

Hellerstein, J.: Toward network data independence. In: *SIGMOD Rec.* vol. 32, no. 3 (2003), S. 34–40. – DOI 10.1145/945721.945730. – ISSN 0163–5808

Helmke et al. 1998

Helmke, R. ; Müller, B. ; Neumann, A.: *Internet-Telefonie zwischen TKG, IuKDG und Mediendienste-Staatsvertrag*. JurPC Web-Dok. 93/1998, Abs. 1 - 49. 1998 http://www.jurpc.de/aufsatz/19980093.htm

Henze & Kadelka 2000

Henze, N. ; Kadelka, D.: *Wahrscheinlichkeitstheorie und Statistik für Studierende der Informatik*. Skript, Universität Karlsruhe (TH), 2000

Heun 2003

Heun, S.-E.: Der Referentenentwurf zur TKG-Novelle. In: *Computer und Recht (CR), Heft 7/2003* (2003), S. 485–496. – ISSN 01791990

Hildrum & Kubiatowicz 2007

Hildrum, K. ; Kubiatowicz, J.: Asymptotically Efficient Approaches to Fault-Tolerance in Peer-to-Peer Networks. In: *Distributed Computing, Proceedings (LNCS 2848)*, Springer, 2007. – DOI 10.1007/b13831. – ISBN 978–3–540–20184–7, S. 321–336

Hoeren 2002

Hoeren, T.: Urheberrecht und Peer-to-Peer-Dienste. In: Schoder, D. (Hrsg.) ; Fischbach, K. (Hrsg.) ; Teischmann, U. (Hrsg.): *Peer-to-Peer. Ökonomische, technologische und juristische Perspektiven*. Springer, 2002. – ISBN 3–540–43708–8, S. 255–294

Hoeren 2007

Hoeren, T.: Das Telemediengesetz. In: *Neue Juristische Wochenschrift (NJW), Heft 12* (2007), S. 801–806. – ISSN 0341–1915

Hoeren 2008

Hoeren, T.: *Internetrecht, Stand: März 2008*. (WWW-Veröffentlichung). 2008 http://www.rtr.at/de/tk/TKG2003

Holz et al. 2008

Holz, T. ; Steiner, M. ; Dahl, F. ; Biersack, E. ; Freiling, F.: Measurements and Mitigation of Peer-to-Peer-based Botnets: A Case Study on Storm Worm. In: *First Usenix Workshop on Large-Scale Exploits and Emergent Threats (LEET'08)*, USENIX Association, 2008

Holznagel & Bonnekoh 2005

Holznagel ; Bonnekoh: Voice over IP - Regulierungsbedarf und erste Lösungen. In: *Multimedia und Recht (MMR), Heft 9* (2005), S. 585–591. – ISSN 1434–596X

Hoschek 2002

Hoschek, W.: A Unified Peer-to-Peer Database Framework for Scalable Service and Resource Discovery. In: *Grid Computing - GRID 2002 (LNCS 2536)*, Springer-Verlag, 2002. – DOI 10.1007/3–540–36133–2. – ISBN 978–3–540–00133–1, S. 126–144

Huang 2007
Huang, G.: *Experiences with PPLive, Keynote at the Peer-to-Peer Streaming and IP-TV Workshop (P2P-TV) in conjunction with ACM Sigcomm 2007*. (WWW-Veröffentlichung). 2007 http://www.sigcomm.org/sigcomm2007/p2p-tv/

Huebsch et al. 2003
Huebsch, R. ; Hellerstein, J. ; Lanham, N. ; Loo, B. T. ; Shenker, S. ; Stoica, I.: Querying the internet with PIER. In: *vldb'2003: Proceedings of the 29th international conference on Very large data bases*, VLDB Endowment, 2003. – ISBN 0–12–722442–4, S. 321–332

Hummel et al. 2005
Hummel, T. ; Muhle, S. ; Schoder, D.: Business Applications and Revenue Models. 2005. In: Steinmetz, R. (Hrsg.) ; Wehrle, K. (Hrsg.): *Peer-to-Peer Systems and Applications (LNCS 3485)*. Springer, 2005. – DOI 10.1007/11530657. – ISBN 3–540–29192–X, S. 437–489

IANA IPv4
IANA: *IPv4 Global Unicast Address Assignments*. (WWW-Veröffentlichung), 2008. http://www.iana.org/assignments/ipv4-address-space

IANA Ports
IANA: *Port Numbers*. (WWW-Veröffentlichung), 2008. http://www.iana.org/assignments/port-numbers

IEEE 1991
IEEE: *IEEE Std. 610-1991: IEEE standard computer dictionary. A compilation of IEEE standard computer glossaries*. 1991

eco Verband der deutschen Internetwirtschaft e.V. 2004
Internetwirtschaft e.V. eco Verband der d.: *Stellungnahme zum Entwurf eines Telekommunikationsgesetzes -TKG (Stand 15.10.2003), Stand 04.02.2004*. (WWW-Veröffentlichung). 2004 http://www.eco.de/dokumente/20040204-ecoStellungnahme-TKG-1.0.pdf

Ipoque 2006
GmbH ipoque: *P2P-Studie 2006*. (WWW-Veröffentlichung). 2006 http://www.ipoque.com/news_&_events/internet_studies/p2p-studie_2006

Ipoque 2007

GmbH ipoque: *Internetstudie 2007*. (WWW-Veröffentlichung). 2007 `http://www.ipoque.com/news_&_events/internet_studies/internet_study_2007`

ISO/IEC 7498-1

ISO/IEC: *7498-1: 1994 – Information processing systems – Open Systems Interconnection – Basic Reference Model: The Basic Model*, 1994

ITU NGN, Study Group 13

ITU-T: *Definition of Next Generation Network*. (WWW-Veröffentlichung), 2008. `http://www.itu.int/ITU-T/studygroups/com13/ngn2004/working_definition.html`

Izal et al. 2004

Izal, M. ; Urvoy-Keller, G. ; Biersack, Ernst ; Felber, P.A. ; Hamra, A. A. ; Garces-Erice, L.: Dissecting BitTorrent: Five Months in a Torrent's Lifetime. In: *Passive and Active Network Measurement (LNCS 3015)*, Springer, 2004. – DOI 10.1007/b96961. – ISBN 978–3–540–21492–2, S. 1–11

Jaeger et al. 2008

Jaeger, M. ; Werner, M. ; Mühl, G. ; Heiss, H.-U. ; Laude, U. ; Ruge, C.: Autonomie in IT-Systemen - Ein konzeptionelles Modell. In: *PIK - Praxis der Informationsverarbeitung und Kommunikation* Jg. 31, Nr. 1 (2008), S. 4–11. – DOI 10.1515/piko.2008.002. – ISSN 1066–8888

Jannotti et al. 2000

Jannotti, J. ; Gifford, D. ; Johnson, K. ; Kaashoek, M. ; J. O'Toole, Jr.: Overcast: reliable multicasting with on overlay network. In: *OSDI'00: Proceedings of the 4th conference on Symposium on Operating System Design & Implementation*, USENIX Association, 2000, S. 14–14

Jelasity et al. 2006

Jelasity, M. ; Montresor, A. ; Babaoglu, O.: The Bootstrapping Service. In: *ICDCSW '06: Proceedings of the 26th IEEE International Conference - Workshops on Distributed Computing Systems*, IEEE Computer Society, 2006. – DOI 10.1109/ICDCSW.2006.105. – ISBN 0–7695–2541–5, S. 11

Jünemann & Dinger 2008

Jünemann, K. ; Dinger, J.: OvlVis: Visualization of Peer-to-Peer networks in simulation and testbed environments. In: *Proceedings of the 11th Communications and Networking Simulation Symposium (CNS'08)*, SCS, 2008. – DOI 10.1145/1400713.1400741. – ISBN 1–56555–318–7, S. 164–171

JXTA Spec 2007

Inc., Sun M.: *JXTA v2.0 Protocols Specification*. (WWW-Veröffentlichung). 2007 https://jxta-spec.dev.java.net/

Kaashoek & Karger 2003

Kaashoek, M. F. ; Karger, D.: Koorde: A Simple Degree-Optimal Distributed Hash Table. In: *Peer-to-Peer Systems II : Second International Workshop, IPTPS 2003 Berkeley, CA, USA, February 21-22, 2003 Revised Papers (LNCS 2735)*, Springer, 2003. – DOI 10.1007/b11823. – ISBN 978–3–540–40724–9, S. 98–107

Kan 2001

Kan, G.: Gnutella. In: Oram, A. (Hrsg.): *Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology*. O'Reilly, 2001. – ISBN 0–596–00110–X, S. 94–122

Karagiannis et al. 2004

Karagiannis, T. ; Broido, A. ; Faloutsos, M. ; Claffy, K.: Transport layer identification of P2P traffic. In: *IMC '04: Proceedings of the 4th ACM SIGCOMM conference on Internet measurement*, ACM, 2004. – DOI 10.1145/1028788.1028804. – ISBN 1–58113–821–0, S. 121–134

Karbhari et al. 2004

Karbhari, P. ; Ammar, M. ; Dhamdhere, A. ; Raj, H. ; Riley, G. ; Zegura, E.: Bootstrapping in Gnutella: A Measurement Study. In: *Passive and Active Network Measurement (LNCS 3015)*, 2004. – DOI 10.1007/b96961. – ISBN 978–3–540–21492–2, S. 22–32

Karger et al. 1997

Karger, D. ; Lehman, E. ; Leighton, T. ; Panigrahy, R. ; Levine, M. ; Lewin, D.: Consistent hashing and random trees: distributed caching protocols for relieving hot spots on the World Wide Web. In: *STOC '97: Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, ACM, 1997. – DOI 10.1145/258533.258660. – ISBN 0–89791–888–6, S. 654–663

Katko 2005

Katko, P.: Voice-over-IP. In: *Computer und Recht (CR), Heft 3/2005* (2005), S. 189–200. – ISSN 01791990

Kephart & Chess 2003

Kephart, J. ; Chess, D.: The Vision of Autonomic Computing. In: *IEEE Computer* vol. 36, no. 1 (2003), S. 41–50. – DOI 10.1109/MC.2003.1160055. – ISSN 0018–9162

Kleinrock 1995

Kleinrock, L.: Nomadic computing — an opportunity. In: *SIGCOMM Comput. Commun. Rev.* vol. 25, no. 1 (1995), S. 36–40. – DOI 10.1145/205447.205450. – ISSN 0146–4833

Klingberg & Manfredi

Klingberg, T. ; Manfredi, R.: *Gnutella 0.6*. (WWW-Veröffentlichung) http://rfc-gnutella.sourceforge.net/src/rfc-0_6-draft.html

Koenig et al. 2003

Koenig, C. ; Kühling, J. ; Braun, J.-D. ; Capito, R. ; Elspass, M. ; Katzschmann, T. ; Koch, A. ; Loetz, S. ; Neumann, A. ; Winkler, K.: *Anmerkungen zum Referentenentwurf zur TKG-Novelle des Bundesministeriums für Wirtschaft und Arbeit (BMWA)*. (WWW-Veröffentlichung). 2003 http://www.tkrecht.de/tkg_novelle/2003/material/zei_20030526.pdf

Koenig & Neumann 1999

Koenig, C. ; Neumann, A.: Internet-Protokoll-Adressen als "Nummernïm Sinne des Telekommunikationsrechts? In: *Kommunikation & Recht (K&R), Heft 4* (1999), S. 145–151. – ISSN 14346354

Koenig & Neumann 2004

Koenig, C. ; Neumann, A.: Telekommunikationsrechtliche Ansprüche auf Leistungen der Fakturierung und des Inkassos für Internet-by-Call-Dienstleistungen. In: *Kommunikation & Recht (K&R), Beilage 3/2004* (2004), S. 1–31. – ISSN 14346354

Kubiatowicz 2003

Kubiatowicz, J.: Extracting guarantees from chaos. In: *Commun. ACM* vol. 46, no. 2 (2003), S. 33–38. – DOI 10.1145/606272.606297. – ISSN 0001–0782

Kubiatowicz et al. 2000

Kubiatowicz, J. ; Bindel, D. ; Chen, Y. ; Czerwinski, S. ; Eaton, P. ; Geels, D. ; Gummadi, R. ; Rhea, S. ; Weatherspoon, H. ; Weimer, W. ; Wells, C. ; Zhao, B.: OceanStore: an architecture for global-scale persistent storage. In: *SIGPLAN Not.* vol. 35, no. 11 (2000), S. 190–201. – DOI 10.1145/356989.357007. – ISSN 0362–1340

Kurose & Ross 2004

Kurose, J. ; Ross, K.: *Computer Networking: A Top-Down Approach Featuring the Internet*. 3rd edition. Addison Wesley, 2004. – ISBN 0–321–26976–4

Kurth 2003

Kurth, M.: Wettbewerb im Internetzugangsmarkt. In: *Multimedia und Recht (MMR), Beilage 3/2003* (2003), S. 3–6. – ISSN 1434–596X

Lakshminarayanan et al. 2005

Lakshminarayanan, K. ; Rangarajan, A. ; Venkatachary, S.: Algorithms for advanced packet classification with ternary CAMs. In: *SIGCOMM '05: Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for*

computer communications, ACM, 2005. – DOI 10.1145/1080091.1080115. – ISBN 1–59593–009–4, S. 193–204

Lamport et al. 1982
Lamport, L. ; Shostak, R. ; Pease, M.: The Byzantine Generals Problem. In: *ACM Trans. Program. Lang. Syst.* vol. 4, no. 3 (1982), S. 382–401. – DOI 10.1145/357172.357176. – ISSN 0164–0925

Leiner et al. 2003
Leiner, B. ; Cerf, V. ; Clark, D. ; Kahn, R. ; Kleinrock, L. ; Lynch, D. ; Postel, J. ; Roberts, L. ; Wolff, S.: *A Brief History of the Internet*. (WWW-Veröffentlichung). 2003 http://www.isoc.org/internet/history/brief.shtml

Lesniewski-Laas 2008
Lesniewski-Laas, C.: A Sybil-proof One-hop DHT. In: *First International Workshop on Social Network Systems, SocialNets'08*, ACM, 2008. – ISBN 978–1–60558–124–8, S. 19–24

Leuf 2002
Leuf, B.: *Peer to peer : collaboration and sharing over the Internet*. Addison-Wesley, 2002. – ISBN 0–201–76732–5

Levine et al. 2006
Levine, B. ; Shields, C. ; Margolin, B.: A Survey of Solutions to the Sybil Attack. 2006. http://prisms.cs.umass.edu/brian/pubs/levine.sybil.tr.2006.pdf. Department of Computer Science, University of Massachusetts Amherst, 2006 (2006-052). – Forschungsbericht

LG Berlin 2002 2003
102/02, LG Berlin 17.09.2002 103 O.: Pflicht zur Anbieterkennzeichnung i.S.d. TDG. In: *Computer und Recht (CR)* (2003), S. 139–141. – ISSN 01791990

Liu et al. 2008
Liu, Y. ; Guo, Y. ; Liang, C.: A survey on peer-to-peer video streaming systems. In: *Peer-to-Peer Networking and Applications* vol. 1, no. 1 (2008), S. 18–28. – DOI 10.1007/s12083–007–0006–y. – ISSN 1936–6442

Loetz & Neumann 2003
Loetz, C. Koenig S. ; Neumann, A.: *tkrecht.de – Kommunikationspolitisches Positionspapier #1: Der Anwendungsbereich des künftigen Telekommunikationsgesetzes*. (WWW-Veröffentlichung). 2003 http://www.tkrecht.de/positionspapiere/positionspapier1.pdf

LT-Drs. 16/1046
Landtag, Schleswig-Holsteinischer: *Entwurf eines Gesetzes zum Neunten Rundfunkänderungsstaatsvertrag*, 2006

Lua et al. 2005

Lua, E. ; Crowcroft, J. ; Pias, M. ; Sharma, R. ; Lim, S.: A survey and comparison of peer-to-peer overlay network schemes. In: *Communications Surveys & Tutorials, IEEE* vol. 7, no. 2 (2005), S. 72–93. – ISSN 1553–877X

Lv et al. 2002

Lv, Q. ; Cao, P. ; Cohen, E. ; Li, K. ; Shenker, S.: Search and replication in unstructured peer-to-peer networks. In: *ICS '02: Proceedings of the 16th international conference on Supercomputing*, ACM, 2002. – DOI 10.1145/514191.514206. – ISBN 1–58113–483–5, S. 84–95

Malkhi et al. 2002

Malkhi, D. ; Naor, M. ; Ratajczak, D.: Viceroy: a scalable and dynamic emulation of the butterfly. In: *PODC '02: Proceedings of the twenty-first annual symposium on Principles of distributed computing*, ACM, 2002. – DOI 10.1145/571825.571857. – ISBN 1–58113–485–1, S. 183–192

Manku et al. 2003

Manku, G. S. ; Bawa, M. ; Raghavan, P.: Symphony: distributed hashing in a small world. In: *USITS'03: Proceedings of the 4th conference on USENIX Symposium on Internet Technologies and Systems*, USENIX Association, 2003

Manssen 2005

Manssen, G.: *Telekommunikations- und Multimediarecht*. Erich Schmidt Verlag, Berlin, 2005. – ISBN 3–503–04817–0

Margolin & Levine 2008

Margolin, B. ; Levine, B.: Quantifying Resistance to the Sybil Attack. In: *Financial Cryptography and Data Security 2008 (FC08), Proc. of the Twelfth International Conference on*, IFCA, 2008

Maymounkov & Mazieres 2002

Maymounkov, P. ; Mazieres, D.: Kademlia: A Peer-to-Peer Information System Based on the XOR Metric. In: *Peer-to-Peer Systems: 1st International Workshop on Peer-to-Peer Systems (IPTPS 2002), Revised Papers (LNCS 2429)*. London, UK : Springer, 2002. – DOI 10.1007/3–540–45748–8. – ISBN 978–3–540–44179–3, S. 53–65

MDStV 97

Staatsvertrag über Mediendienste (Mediendienstestaatsvertrag - MDStV), vom 20. Januar bis 12. Februar 1997, in der Fassung des 6. Rundfunkänderungsstaatsvertrages vom 19.06.2002 (Nds. GVBl. Nr. 16/2002 S. 175), geändert durch § 25 Abs. 4 des JMStV vom 10.-27.9.2002 (Nds.GVBI. Nr. 31/2002 S. 706) und Art. 8 des 8. Rundfunkänderungsstaatsvertrages vom

25.2.2005 (Nds. GVBl. Nr. 5/2005 S. 61)
http://www.recht-niedersachsen.de/22620/mdstv1.htm

Meinberg & Grabe 2004
Meinberg, R. ; Grabe, O.: Voice over IP - IP basierter Sprachdienst vor dem Hintergrund des novellierten TKG. In: *Kommunikation & Recht (K&R), Heft* (2004), S. 409–417. – ISSN 14346354

Merkle 1978
Merkle, R.: Secure communications over insecure channels. In: *Commun. ACM* vol. 21, no. 4 (1978), S. 294–299. – DOI 10.1145/359460.359473. – ISSN 0001–0782

Meuer 2008
Meuer, H.: The TOP500 Project: Looking Back Over 15 Years of Supercomputing Experience. In: *Informatik-Spektrum* Jg. 31, Nr. 3 (2008), S. 203–222. – DOI 10.1007/s00287–008–0240–6. – ISSN 1432–122X

Miller 2001
Miller, M.: *Discovering P2P*. Alameda, CA, USA : SYBEX Inc., 2001. – ISBN 0782140181

Milojicic et al. 2002
Milojicic, D. ; Kalogeraki, V. ; Lukose, R. ; Nagaraja, K. ; Pruyne, J. ; Richard, B. ; Rollins, S. ; Xu, Z.: Peer-to-Peer Computing. 2002. http://www.hpl.hp.com/techreports/2002/HPL-2002-57R1.html. HP Laboratories Palo Alto, 2002 (HPL-2002-57R1). – Forschungsbericht

Minar & Hedlund 2001
Minar, N. ; Hedlund, M.: A Network of Peers – Peer-to-Peer Models Through the History of the Internet. In: Oram, A. (Hrsg.): *Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology*. O'Reilly, 2001. – ISBN 0–596–00110–X, S. 3–20

Mischke & Stiller 2004
Mischke, J. ; Stiller, B.: A Methodology for the Design of Distributed Search in P2P Middleware. In: *Network, IEEE* vol. 18, no. 1 (2004), S. 30–37. – DOI 10.1109/MNET.2004.1265831. – ISSN 0890–8044

Möller 2000
Möller, H.: Gesetzliche Vorgaben für anonyme E-Mail. In: *Datenschutz und Datensicherheit (DuD), Heft 6* (2000), S. 344–348. – ISSN 0724–4371

Mockapetris & Dunlap 1995
Mockapetris, Paul V. ; Dunlap, Kevin J.: Development of the Domain Name System. In: *SIGCOMM Comput. Commun. Rev.* vol. 25, no. 1 (1995), S. 112–122. – DOI 10.1145/205447.205459. – ISSN 0146–4833

Moore & Hebeler 2001

Moore, D. ; Hebeler, J.: *Peer-to-Peer: Building Secure, Scalable, and Manageable Networks*. McGraw-Hill Companies, 2001. – ISBN 0072192844

MS Pnrp 2006

Corp., Microsoft: *Peer-to-peer name resolution protocol (PNRP) and multilevel cache for use therewith* . United States Patent 7,065,587. 2006 http://patft.uspto.gov/netacgi/nph-Parser?patentnumber=7065587

Naoumov & Ross 2006

Naoumov, N. ; Ross, K.: Exploiting P2P systems for DDoS attacks. In: *InfoScale '06: Proceedings of the 1st international conference on Scalable information systems*, ACM, 2006. – DOI 10.1145/1146847.1146894. – ISBN 1–59593–428–6

Naraghi-Pour et al. 1998

Naraghi-Pour, M. ; Hegde, M. ; Pallapotu, R.: Peer-to-peer communication in wireless local area networks. In: *Computer Communications and Networks, 1998. Proceedings. 7th International Conference on*, 1998. – DOI 10.1109/ICCCN.1998.739946. – ISBN 0–8186–9014–3, S. 432–439

Newsome et al. 2004

Newsome, J. ; Shi, E. ; Song, D. ; Perrig, A.: The sybil attack in sensor networks: analysis & defenses. In: *IPSN '04: Proceedings of the third international symposium on Information processing in sensor networks*, ACM, 2004. – DOI 10.1145/984622.984660. – ISBN 1–58113–846–6, S. 259–268

Oasis UDDI

Organization for the Advancement of Structured Information Standards (OASIS): *OASIS UDDI Specification TC*, 2008. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=uddi-spec

Oasis WSS

Organization for the Advancement of Structured Information Standards (OASIS): *OASIS Web Services Security (WSS) TC*, 2008. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

OLG Hamburg 2002 2003

8o/o2, OLG Hamburg 20.11.2002 5 W.: OLG Hamburg: Impressums- und Kennzeichnungspflichten. In: *Multimedia und Recht (MMR), Heft 2/2003* (2003), S. 105–108. – ISSN 1434–596X

Oram 2001

Oram, A. (Hrsg.): *Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology*. O'Reilly, 2001. – ISBN 0–596–00110–X

Papazoglou & Heuvel 2007

Papazoglou, M. ; Heuvel, W.: Service oriented architectures: approaches, technologies and research issues. In: *The VLDB Journal* vol. 16, no. 3 (2007), S. 389–415. – DOI 10.1007/s00778–007–0044–3. – ISSN 1066–8888

Parameswaran et al. 2001

Parameswaran, M. ; Susarla, A. ; Whinston, A.: P2P Networking: An Information-Sharing Alternative. In: *Computer* vol. 34, no. 7 (2001), S. 31–38. – DOI 10.1109/2.933501. – ISSN 0018–9162

Pavlov & Saeed 2004

Pavlov, O. ; Saeed, K.: A Resource-Based Analysis of Peer-to-Peer Technology. In: *System Dynamics Review* vol. 20, no. 3 (2004), S. 237–262. – DOI 10.1002/sdr.297. – ISSN 1099–1727

Peterson & Davie 2003

Peterson, L. ; Davie, B.: *Computer Networks: A System Approach*. 3rd edition. Morgan Kaufmann, 2003. – ISBN 1–55860–833–8

Piro et al. 2006

Piro, C. ; Shields, C. ; Levine, B.: Detecting the Sybil Attack in Mobile Ad hoc Networks. In: *Securecomm and Workshops, 2006*, 2006. – DOI 10.1109/SECCOMW.2006.359558. – ISBN 1–4244–0423–1, S. 1–11

Plaxton et al. 1997

Plaxton, C. ; Rajaraman, R. ; Richa, A.: Accessing nearby copies of replicated objects in a distributed environment. In: *SPAA '97: Proceedings of the ninth annual ACM symposium on Parallel algorithms and architectures*. New York, NY, USA : ACM, 1997. – DOI 10.1145/258492.258523. – ISBN 0–89791–890–8, S. 311–320

Pras et al. 2007

Pras, A. ; Schönwälder, J. ; Stiller, B.: Peer-to-Peer Technologies in Network and Service Management. In: *J. Netw. Syst. Manage.* vol. 15, no. 3 (2007), S. 285–288. – DOI 10.1007/s10922–007–9072–y. – ISSN 1064–7570

Qiao & Bustamante 2006

Qiao, Y. ; Bustamante, F.: Structured and unstructured overlays under the microscope: a measurement-based view of two P2P systems that people use. In: *ATEC '06: Proceedings of the annual conference on USENIX '06 Annual Technical Conference*, USENIX Association, 2006

Raabe 2003

Raabe, O.: Wie Können die Regelungsbereiche des Teledienstерechts zum Telekommunikationsrecht horizontal voneinander abgegrenzt werden? In: *Computer und Recht (CR), Heft 4/2003* (2003), S. 268–273. – ISSN 01791990

Raabe & Dinger 2007
Raabe, O. ; Dinger, J.: Telemedienrechtliche Informationspflichten in P2P-Overlay-Netzen und bei Web-Services. In: *Computer und Recht (CR), Heft 12/2007* (2007), S. 791–797. – ISSN 01791990

Raabe et al. 2007
Raabe, O. ; Dinger, J. ; Hartenstein, H.: Telekommunikationsdienste in Next-Generation-Networks am Beispiel von Peer-to-Peer-Overlay-Systemen. In: *Kommunikation & Recht (K&R), Beihefter 1/2007* (2007), S. 1–12. – ISSN 14346354

Rajab et al. 2007
Rajab, M. ; Zarfoss, J. ; F.Monrose ; Terzis, A.: My botnet is bigger than yours (maybe, better than yours): why size estimates remain challenging. In: *HotBots'07: Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets*, USENIX Association, 2007

Ratnasamy et al. 2001a
Ratnasamy, S. ; Francis, P. ; Handley, M. ; Karp, R. ; Schenker, S.: A scalable content-addressable network. In: *SIGCOMM '01: Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications*, ACM, 2001. – DOI 10.1145/383059.383072. – ISBN 1–58113–411–8, S. 161–172

Ratnasamy et al. 2001b
Ratnasamy, S. ; Handley, M. ; Karp, R. ; Shenker, S.: Application-Level Multicast Using Content-Addressable Networks. In: *NGC '01: Proceedings of the Third International COST264 Workshop on Networked Group Communication*, Springer, 2001. – DOI 10.1007/3–540–45546–9_2. – ISBN 3–540–42824–0, S. 14–29

RFC 2616
Fielding, R. ; Gettys, J. ; Mogul, J. ; Frystyk, H. ; Masinter, L. ; Leach, P. ; Berners-Lee, T.: *Hypertext Transfer Protocol – HTTP/1.1*. RFC 2616 (Draft Standard), Internet Engineering Task Force (IETF), 1999. `http://www.ietf.org/rfc/rfc2616.txt`

RFC 2663
Srisuresh, P. ; Holdrege, M.: *IP Network Address Translator (NAT) Terminology and Considerations*. RFC 2663 (Informational), Internet Engineering Task Force (IETF), 1999. `http://www.ietf.org/rfc/rfc2663.txt`

RFC 2827
Ferguson, P. ; Senie, D.: *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*. RFC 2827 (Best Current Practice),

Internet Engineering Task Force (IETF), 2000.
http://www.ietf.org/rfc/rfc2827.txt

RFC 3261

Rosenberg, J. ; Schulzrinne, H. ; Camarillo, G. ; Johnston, A. ; Peterson, J. ; Sparks, R. ; Handley, M. ; Schooler, E.: *SIP: Session Initiation Protocol*. RFC 3261 (Proposed Standard), Internet Engineering Task Force (IETF), 2002. http://www.ietf.org/rfc/rfc3261.txt

RFC 3263

Rosenberg, J. ; Schulzrinne, H.: *Session Initiation Protocol (SIP): Locating SIP Servers*. RFC 3263 (Proposed Standard), Internet Engineering Task Force (IETF), 2002. http://www.ietf.org/rfc/rfc3263.txt

RFC 3330

IANA: *Special-Use IPv4 Addresses*. RFC 3330 (Informational), Internet Engineering Task Force (IETF), 2002. http://www.ietf.org/rfc/rfc3330.txt

RFC 3489

Rosenberg, J. ; Weinberger, J. ; Huitema, C. ; Mahy, R.: *STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)*. RFC 3489 (Proposed Standard), Internet Engineering Task Force (IETF), 2003. http://www.ietf.org/rfc/rfc3489.txt

RFC 3986

Berners-Lee, T. ; Fielding, R. ; Masinter, L.: *Uniform Resource Identifier (URI): Generic Syntax*. RFC 2616 (Draft Standard), Internet Engineering Task Force (IETF), 2005. http://www.ietf.org/rfc/rfc3986.txt

RFC 4291

Hinden, R. ; Deering, S.: *IP Version 6 Addressing Architecture*. RFC 4291 (Draft Standard), Internet Engineering Task Force (IETF), 2006.
http://www.ietf.org/rfc/rfc4291.txt

RFC 4941

Narten, T. ; Draves, R. ; Krishnan, S.: *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*. RFC 4941 (Draft Standard), Internet Engineering Task Force (IETF), 2007. http://www.ietf.org/rfc/rfc4941.txt

RFC 4981

Risson, J. ; Moors, T.: *Survey of Research towards Robust Peer-to-Peer Networks: Search Methods*. RFC 4981 (Informational), Internet Engineering Task Force (IETF), 2007. http://www.ietf.org/rfc/rfc4981.txt

Rhea et al. 2005a

Rhea, S. ; Chun, B.-G. ; Kubiatowicz, J. ; Shenker, S.: Fixing the embarrassing slowness of OpenDHT on PlanetLab. In: *WORLDS'05: Proceedings of the 2nd conference on Real, Large Distributed Systems*, USENIX Association, 2005

Rhea et al. 2004

Rhea, S. ; Geels, D. ; Roscoe, T. ; Kubiatowicz, J.: Handling churn in a DHT. In: *ATEC '04: Proceedings of the annual conference on USENIX Annual Technical Conference*, USENIX Association, 2004, S. 127–140

Rhea et al. 2005b

Rhea, S. ; Godfrey, B. ; Karp, B. ; Kubiatowicz, J. ; Ratnasamy, S. ; Shenker, S. ; Stoica, I. ; Yu, H.: OpenDHT: a public DHT service and its uses. In: *SIGCOMM '05: Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications*, ACM, 2005. – DOI 10.1145/1080091.1080102. – ISBN 1–59593–009–4, S. 73–84

Richtel 2000

Richtel, M.: *In Victory for Recording Industry, Judge Bars Online Music Sharing.* (WWW-Veröffentlichung). 2000
`http://query.nytimes.com/gst/fullpage.html?res=9C00E3D61F3AF934A15754C0A9669C8B63&sec=&spon=&partner=permalink&exprod=permalink`

Ripeanu 2001

Ripeanu, M.: Peer-to-peer architecture case study: Gnutella network. In: *Peer-to-Peer Computing, 2001. Proceedings. First International Conference on* (2001), S. 99–100. – DOI 10.1109/P2P.2001.990433. ISBN 0–7695–1503–7

Risson & Moors 2006

Risson, J. ; Moors, T.: Survey of research towards robust peer-to-peer networks: search methods. In: *Comput. Netw.* vol. 50, no. 17 (2006), S. 3485–3521. – DOI 10.1016/j.comnet.2006.02.001. – ISSN 1389–1286

Rodrigues & Liskov 2005

Rodrigues, R. ; Liskov, B.: High Availability in DHTs: Erasure Coding vs. Replication. In: *Peer-to-Peer Systems IV : 4th International Workshop, IPTPS 2005, Ithaca, NY, USA, February 24-25, 2005. Revised Selected Papers (LNCS 3640)*, Springer, 2005. – DOI 10.1007/11558989. – ISBN 978–3–540–29068–1, S. 226–239

Rodrigues et al. 2002

Rodrigues, R. ; Liskov, B. ; Shrira, L.: The design of a robust peer-to-peer system. In: *EW10: Proceedings of the 10th workshop on ACM SIGOPS European workshop*, ACM, 2002. – DOI 10.1145/1133373.1133396, S. 117–124

Roßnagel 2005

Rossnagel, A.: *Recht der Multimedia-Dienste: Kommentar zum IuKDG und zum MDStV*. C. H. Beck, 2005. – ISBN 978–3–406–44463–0

Rossi et al.

Rossi, D. ; Mellia, M. ; Meo, M.: *A Detailed Measurement of Skype Network Traffic*. 7th International Workshop on Peer-to-Peer Systems, IPTPS 2008 (WWW-Veröffentlichung), 2008. http://www.cs.toronto.edu/iptps2008/final/31.pdf

Roussopoulos et al. 2005

Roussopoulos, M. ; Baker, M. ; Rosenthal, D. ; Giuli, T. ; Maniatis, P. ; Mogul, J.: 2 P2P or Not 2 P2P? In: *Peer-to-Peer Systems III : Third International Workshop, IPTPS 2004, La Jolla, CA, USA, February 26-27, 2004, Revised Selected Papers (LNCS 3279)*, Springer, 2005. – DOI 10.1007/b104020. – ISBN 978–3–540–24252–9, S. 33–43

Rowaihy et al. 2005

Rowaihy, H. ; Enck, W. ; McDaniel, P. ; La Porta, T.: Limiting Sybil Attacks in Structured Peer-to-Peer Networks / Network and Security Research Center. 2005. http://nsrc.cse.psu.edu/tech_report/NAS-TR-0017-2005.pdf. Department of Computer Science and Engineering, Pennsylvania State University, 2005 (NAS-TR-0017-2005). – Forschungsbericht

Rowaihy et al. 2007

Rowaihy, H. ; Enck, W. ; McDaniel, P. ; Porta, T. L.: Limiting Sybil Attacks in Structured P2P Networks. In: *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, IEEE, 2007. – DOI 10.1109/INFCOM.2007.328. – ISSN 0743–166X, S. 2596–2600

Rowstron & Druschel 2001

Rowstron, A. ; Druschel, P.: Pastry: Scalable, Decentralized Object Location, and Routing for Large-Scale Peer-to-Peer Systems. In: *Middleware '01: Proceedings of the IFIP/ACM International Conference on Distributed Systems Platforms Heidelberg*, Springer-Verlag, 2001. – ISBN 3–540–42800–3, S. 329–350

RStV 2007

Staatsvertrag für Rundfunk und Telemedien (Rundfunkstaatsvertrag - RStV) vom 31.08.1991, zuletzt geändert durch Artikel 1 des Neunten Staatsvertrages zur nderung rundfunkrechtlicher Staatsverträge vom 31.07. bis 10.10.2006 (GBl. BW 2007 S. 111), in Kraft getreten am 01.03.2007 http://www.lfk.de/gesetzeundrichtlinien/rundfunkstaatsvertrag/main.html

RTR 2006

GmbH, RTR: *Voice over IP: Grundlagen, Regulierung und erste Erfahrungen*. Schriftenreihe der Rundfunk und Telekom Regulierungs-GmbH, Band 1/2006. 2006 http://www.rtr.at/de/komp/SchriftenreiheNr12006

Röttgers 2003

Röttgers, Janko: *Mix, Burn & R.I.P. : Das Ende der Musikindustrie*. Verlag Heinz Heise, 2003. – ISBN 3–936931–08–9

Sahin et al. 2005

Sahin, O. ; Gerede, C. ; Agrawal, D. ; Abbadi, A. ; Ibarra, O. ; Su, J.: SPiDeR: P2P-Based Web Service Discovery. In: *Proceedings of the Third International Conference on Service-Oriented Computing - ICSOC 2005 (LNCS 3826)*, Springer-Verlag, 2005. – DOI 10.1007/11596141. – ISBN 978–3–540–30817–1, S. 157–169

Saltzer et al. 1984

Saltzer, J. ; Reed, D. ; Clark, D.: End-to-end arguments in system design. In: *ACM Trans. Comput. Syst.* vol. 2, no. 4 (1984), S. 277–288. – DOI 10.1145/357401.357402. – ISSN 0734–2071

Sartre 1943

Sartre, J.-P.: *Das Sein und das Nichts: Versuch einer phänomenologischen Ontologie*. Rowohlt, 1943. – ISBN 3–498–06262–X. – Übersetzung: H. Schöneberg u. T. König, 1991

v. Schewick 2005

Schewick, B. v.: *Architecture & innovation : the role of the end-to-end arguments in the original internet, Diss., Technischen Universität Berlin*. 2005

Schiller 2000

Schiller, J.: *Mobilkommunikation : Techniken für das allgegenwärtige Internet*. Addison-Wesley, 2000. – ISBN 3–8273–1578–6

Schlichting & Schneider 1983

Schlichting, R. ; Schneider, F.: Fail-stop processors: an approach to designing fault-tolerant computing systems. In: *ACM Trans. Comput. Syst.* vol. 1, no. 3 (1983), S. 222–238. – DOI 10.1145/357369.357371. – ISSN 0734–2071

Schlosser et al. 2002

Schlosser, M. ; Sintek, M. ; Decker, S. ; Nejdl, W.: HyperCuP — Hypercubes, Ontologies, and Efficient Search on Peer-to-Peer Networks. In: *Agents and Peer-to-Peer Computing: First International Workshop, AP2PC 2002, Bologna, Italy, July 15, 2002, Revised and Invited Papers (LNCS 2530)*, Springer, 2002. – DOI 10.1007/3–540–45074–2. – ISBN 978–3–540–40538–2, S. 112–125

Schoder & Fischbach 2003
Schoder, D. ; Fischbach, K.: Peer-to-Peer-Netzwerke für das Ressourcenmanagement. In: *Wirtschaftsinformatik* vol. 45, no. 3 (2003), S. 313–323. – ISSN 0937–6429

Schoder et al. 2002
Schoder, D. (Hrsg.) ; Fischbach, K. (Hrsg.) ; Teichmann, R. (Hrsg.): *Peer-to-Peer: Ökonomische, technische und juristische Perspektiven, Das aktuelle P2P-Buch*. Springer, 2002. – ISBN 3–540–43708–8

Schramm 2004
Schramm: Pflicht zur Anbieterkennzeichnung. In: *Datenschutz und Datensicherheit (DuD), Heft 8* (2004), S. 472–475. – ISSN 0724–4371

Schreiber 1995
Schreiber, F.: *Sybil*. Warner Books, 1995. – ISBN 978–9995442453

Science & Board 1994
Science, Corporate C. ; Board, Telecommunications: *"Realizing the Information Future: The Internet and Beyond"*. National Academy Press, 1994. – ISBN 0–309–05044–8

Seitlinger & Strobl 2005
Seitlinger, M. ; Strobl, K.: *Voice over IP – eine rechtliche Beurteilung vom Kommunikationsdienst bis zum Netzzugang*. (WWW-Veröffentlichung). 2005 `http://www.it-law.at/uploads/tx_publications/Voice_over_IP__eine_rechtliche_Beurteilung_vom_Kommunikationsdienst_bis_zum_Netzzugang.pdf`

Sen & Wang 2002
Sen, S. ; Wang, J.: Analyzing peer-to-peer traffic across large networks. In: *IMW '02: Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment*, ACM, 2002. – DOI 10.1145/637201.637222. – ISBN 1–58113–603–X, S. 137–150

Shirky 2001
Shirky, C.: Listening to Napster. In: Oram, A. (Hrsg.): *Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology*. O'Reilly, 2001. – ISBN 0–596–00110–X, S. 31–37

Simon 1991
Simon, S.: Peer-to-peer network management in an IBM SNA network. In: *Network, IEEE* vol. 5, no. 2 (1991), S. 30–34. – ISSN 0890–8044

Singh et al. 2004

Singh, A. ; Castro, M. ; Druschel, P. ; Rowstron, A.: Defending against eclipse attacks on overlay networks. In: *EW11: Proceedings of the 11th workshop on ACM SIGOPS European workshop*, ACM, 2004. – DOI 10.1145/1133572.1133613, S. 21

Singh 2001
Singh, M.: Peering at peer-to-peer computing. In: *IEEE Internet Computing* vol. 5, no. 6 (2001), S. 4–5. – DOI 10.1109/MIC.2001.968826. – ISSN 1089–7801

Singla & Rohrs 2002
Singla, A. ; Rohrs, C.: *Ultrapeers: Another Step Towards Gnutella Scalability, Version 1.0*. (WWW-Veröffentlichung). 2002
`http://www.limewire.com/developer/Ultrapeers.html`

Sit & Morris 2002
Sit, E. ; Morris, R.: Security Considerations for Peer-to-Peer Distributed Hash Tables. In: *Peer-to-Peer Systems: 1st International Workshop on Peer-to-Peer Systems (IPTPS 2002), Revised Papers (LNCS 2429)*, Springer, 2002. – DOI 10.1007/3–540–45748–8. – ISBN 978–3–540–44179–3, S. 261–269

SOA Oasis
OASIS (Organization for the Advancement of Structured Information Standards): *OASIS Reference Model for Service Oriented Architecture 1.0*. (WWW-Veröffentlichung), 2006. `http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=soa-rm`

Spies 2006
Spies: USA: Kampf um die Netzneutralität. In: *Multimedia und Recht (MMR), Heft 8* (2006), S. XXI–XIII. – ISSN 1434–596X

Sripanidkulchai 2001
Sripanidkulchai, K.: *The popularity of Gnutella queries and its implications on scalability*. (WWW-Veröffentlichung). 2001
`http://www.cs.cmu.edu/~kunwadee/research/p2p/paper.html`

Steiner et al. 2007
Steiner, M. ; En-Najjary, T. ; Biersack, E.: A global view of kad. In: *IMC '07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, 2007. – DOI 10.1145/1298306.1298325. – ISBN 978–1–59593–908–1, S. 117–122

Steinmetz & Wehrle 2004
Steinmetz, R. ; Wehrle, K.: Peer-to-Peer Networking & -Computing. In: *Informatik-Spektrum* vol. 27, no. 1 (2004), S. 51–54. – DOI 10.1007/s00287–003–0362–9. – ISSN 1432–122X

Steinmetz & Wehrle 2005a

Steinmetz, R. (Hrsg.) ; Wehrle, K. (Hrsg.): *Peer-to-Peer Systems and Applications (LNCS 3485)*. Springer, 2005. – ISBN 3–540–29192–X

Steinmetz & Wehrle 2005b

Steinmetz, R. ; Wehrle, K.: What Is This "Peer-to-Peer" About? 2005. In: Steinmetz, R. (Hrsg.) ; Wehrle, K. (Hrsg.): *Peer-to-Peer Systems and Applications (LNCS 3485)*. Springer, 2005. – DOI 10.1007/11530657. – ISBN 3–540–29192–X, S. 9–16

Stiller & Mischke 2005

Stiller, B. ; Mischke, J.: Peer-to-Peer Search and Scalability. 2005. In: Steinmetz, R. (Hrsg.) ; Wehrle, K. (Hrsg.): *Peer-to-Peer Systems and Applications (LNCS 3485)*. Springer, 2005. – DOI 10.1007/11530657. – ISBN 3–540–29192–X, S. 269–288

Stoica et al. 2002

Stoica, I. ; Adkins, D. ; Zhuang, S. ; Shenker, S. ; Surana, S.: Internet indirection infrastructure. In: *SIGCOMM Comput. Commun. Rev., Proceedings of the 2002 SIGCOMM conference* vol. 32, no. 4 (2002), S. 73–86. – DOI 10.1145/964725.633033. – ISSN 0146–4833

Stoica et al. 2001

Stoica, I. ; Morris, R. ; Karger, D. ; Kaashoek, M. ; Balakrishnan, H.: Chord: A scalable peer-to-peer lookup service for internet applications. In: *SIGCOMM Comput. Commun. Rev.* vol. 31, no. 4 (2001), S. 149–160. – DOI 10.1145/964723.383071. – ISSN 0146–4833

Stutzbach & Rejaie 2006a

Stutzbach, D. ; Rejaie, R.: Improving Lookup Performance Over a Widely-Deployed DHT. In: *INFOCOM 2006: Proceedings of the 25th IEEE International Conference on Computer Communications*, IEEE, 2006. – DOI 10.1109/INFOCOM.2006.329. – ISBN 1–4244–0221–2, S. 2884–2895

Stutzbach & Rejaie 2006b

Stutzbach, D. ; Rejaie, R.: Understanding churn in peer-to-peer networks. In: *IMC '06: Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*, 2006. – DOI 10.1145/1177080.1177105. – ISBN 1–59593–561–4, S. 189–202

T. Condie et al. 2006

T. Condie, V. K. ; Sankararaman, S. ; Hellerstein, J. ; Maniatis, P.: Induced Churn as Shelter from Routing-Table Poisoning. In: *ISOC, The 13th Annual Network and Distributed System Security Symposium (NDSS06)*, ISOC, 2006. – ISBN 1–891562–22–3

Tanenbaum 2003

Tanenbaum, A.: *Computer Networks*. 4th edition. Pearson Education Inc., Prentice Hall PTR, 2003. – ISBN 0–13–038488–7

TDG 97

Gesetz über die Nutzung von Telediensten (Teledienstegesetz - TDG) vom 22.07.1997 (BGBl. I S. 1870); zuletzt geändert durch Artikel 12 Abs. 15 G. vom 10.11.2006 BGBl. I S. 2553; aufgehoben durch Artikel 5 G. vom 26.02.2007 (BGBl. I S. 179)

TKG 2004

Telekommunikationsgesetz (TKG) vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 2 des Gesetzes vom 21. Dezember 2007 (BGBl. I S. 3198) http://www.bundesrecht.juris.de/tkg_2004/

TKG aF

Telekommunikationsgesetz (TKG) vom 25. Juli 1996 (BGBl. I S. 1120), zuletzt geändert durch Gesetz vom 17.12.97 (BGBl. I 1997 S. 3108) http://archiv.jura.uni-saarland.de/BGBl/TEIL1/1996/19961120.A10.HTML

TKG-Oe

Österreichisches Telekommunikationsgesetz 2003 (TKG 2003), Stammfassung: BGBl. I Nr. 70/2003, Bundesgesetz, idF BGBl I Nr. 133/2005
http://www.rtr.at/de/tk/TKG2003

TKÜV 2005

Telekommunikations-Überwachungsverordnung (TKÜV) vom 3. November 2005 (BGBl. I S. 3136), geändert durch Artikel 13 des Gesetzes vom 21. Dezember 2007 (BGBl. I S. 3198) http://www.gesetze-im-internet.de/tk_v_2005/

TMG 2007

Telemediengesetz (TMG) vom 26. Februar 2007 (BGBl. I S. 179)
http://www.bundesrecht.juris.de/tmg/

TMG-E

BT-Drs. 16/3078, Entwurf eines Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz – ElGVG), 2006.
http://dip.bundestag.de/btd/16/030/1603078.pdf

Traversat et al. 2003

Traversat, B. ; Arora, A. ; Abdelaziz, M. ; Duigou, M. ; Haywood, C. ; Hugly, J.-C. ; Pouyoul, E. ; Yeager, B.: Project JXTA 2.0 Super-Peer Virtual Network. 2003. http://research.sun.com/spotlight/misc/jxta.pdf. Sun Microsystems, Inc., 2003. – Forschungsbericht

(VAT) 2005
(VAT), Verband Alternativer Telekom-Netzbetreiber: *Stellungnahme, Konsultation "Guidelines for VoIP Service Providers"*. (WWW-Veröffentlichung). 2005 http://www.vat.at/VAT-StN_Guidelines_VoIP_Betreiber_08_06_05_endg.pdf

VG Köln 2002
Köln, VG: Urteil, Aktenzeichen: 1 K 2788/00. In: *Neue Zeitschrift für Verwaltungsrecht (NVwZ), Heft 3/2005* (2002). – ISSN 0721–880X

von Ahn et al. 2004
von Ahn, L. ; Blum, M. ; Langford, J.: Telling humans and computers apart automatically. In: *Commun. ACM* vol. 47, no. 2 (2004), S. 56–60. – DOI 10.1145/966389.966390. – ISSN 0001–0782

Vu et al. 2006
Vu, L.-H. ; Hauswirth, M. ; Aberer, K.: Towards P2P-Based Semantic Web Service Discovery with QoS Support. In: *Business Process Management Workshops, BPM 2005 International Workshops BPI, BPD, ENEI, BPRM, WSCOBPM, BPS, Revised Selected Papers (LNCS 3812)*, Springer-Verlag, 2006. – DOI 10.1007/11678564. – ISBN 978–3–540–32595–6, S. 18–31

W3C Soap
World Wide Web Consortium (W3C): *XML Protocol Working Group – SOAP*, 2008. http://www.w3.org/2000/xp/Group/

W3C Soap 1.2
World Wide Web Consortium (W3C): *SOAP Version 1.2 Part 0: Primer (Second Edition)*, 2008. http://www.w3.org/TR/soap12-part0/

W3C wsa
World Wide Web Consortium (W3C): *Web Services Architecture, W3C Working Group Note 11 February 2004*. (WWW-Veröffentlichung), 2004. http://www.w3.org/TR/ws-arch/

W3C Wsdl
World Wide Web Consortium (W3C): *Web Services Description Working Group – WSDL*, 2008. http://www.w3.org/2002/ws/desc/

Waldman et al. 2000
Waldman, M. ; Rubin, A. ; Cranor, L.: Publius: a robust, tamper-evident, censorship-resistant web publishing system. In: *SSYM'00: Proceedings of the 9th conference on USENIX Security Symposium*, USENIX Association, 2000, S. 59–72

Wehrle et al. 2005

Wehrle, K. ; Götz, S. ; Rieche, S.: Distributed Hash Tables. 2005. In: Steinmetz, R. (Hrsg.) ; Wehrle, K. (Hrsg.): *Peer-to-Peer Systems and Applications (LNCS 3485)*. Springer, 2005. – DOI 10.1007/11530657. – ISBN 3–540–29192–X, S. 79–93

Wenzl 2005

Wenzl, F.: *Musiktauschbörsen im Internet : Haftung und Rechtsschutz nach deutschem und amerikanischem Urheberrecht, Diss.* Nomos Verlag, Baden-Baden, 2005. – ISBN 3–8329–1391–2

Woitke 2003a

Woitke, T.: Informationspflichten im Internet und ihre Erfüllung durch das Setzen von Hyperlinks. In: *Wettbewerb in Recht und Praxis (WRP)* (2003), S. 945–955. – ISSN 0172–049X

Woitke 2003b

Woitke, T.: Das "Wie" der Anbieterkennzeichnung gemäß § 6 TDG. In: *Neue Juristische Wochenschrift (NJW)* (2003), S. 871–873. – ISSN 0341–1915

WWW ACM Faq

ACM Portal: Using The Guide - Frequently Asked Questions (FAQs). (WWW-Veröffentlichung), 2008. `http://portal.acm.org/faq_guide.cfm`

WWW ACM Portal

ACM Portal, 2008. `http://portal.acm.org/`

WWW Axis

Apache Axis Project, The Apache Software Foundation, 2008. `http://ws.apache.org/axis/`

WWW Azureus

Website von Azureus: Java BitTorrent Client, 2008. `http://azureus.sourceforge.net/`

WWW Bamboo

Website der Bamboo Distributed Hash Table, 2008. `http://bamboo-dht.org/`

WWW BitT Dev

Entwicklerforum für das BitTorrent Protokoll, 2008. `http://www.bittorrent.org/`

WWW BitTorrent

Website von BitTorrent, 2008. `http://www.bittorrent.com/`

WWW Captcha
Website des Projektes CAPTCHA, 2008. http://www.captcha.net/

WWW Cfp
Hausheer, D.: *List of Peer-to-Peer (P2P) Conferences and Journals*. (WWW-Veröffentlichung), 2008. http://hausheer.osola.com/cfps

WWW Coral
Website des Coral Content Distribution Network, 2008. http://www.coralcdn.org/

WWW eComm
eCommunications – Regulatory framework for telecoms in the European Union, 2008. http://ec.europa.eu/information_society/policy/ecomm/index_en.htm

WWW eMule
eMule Website, 2008. http://www.emule-project.net

WWW IdM-GSI
Website der Identity Management Global Standards Initiative (IdM-GSI) der International Telecommunication Union (ITU), 2008. ITU(InternationalTelecommunicationUnion)

WWW IEEE Faq
IEEE Xplore: What is IEEE Xplore? - Frequently Asked Questions (FAQ). (WWW-Veröffentlichung), 2008. http://ieeexplore.ieee.org/guide/g_oview_faq.jsp

WWW IEEE Xpl
IEEE Xplore, 2008. http://ieeexplore.ieee.org/

WWW IETF
Website der Internet Engineering Task Force (IETF), 2008. http://www.ietf.org/

WWW In2movies
in2movies Website, 2008. http://www.in2movies.de

WWW Iris
Website des Projekts IRIS (Infrastructure for Resilient Internet Systems), 2008. http://www.project-iris.net/

WWW Joost
Website von Joost, 2008. http://www.joost.com/

WWW libTorrent a
libTorrent, DHT-Extensions: Client Identification, 2008. http://rasterbar.com/products/libtorrent/dht_extensions.html

WWW libTorrent b
Website von libTorrent, 2008. http://www.rasterbar.com/products/libtorrent/

WWW MaxMind
Website von MaxMind GeoIP, 2008. http://www.maxmind.com/app/ip-location

WWW MediaDefender
Website von MediaDefender, Inc., 2008. http://www.mediadefender.com/

WWW MS p2p 2008
Inc., Microsoft: *Windows Peer-to-Peer Networking Website*. 2008 http://www.microsoft.com/windowsxp/p2p/default.mspx

WWW OMG
Website der Object Management Group (OMG), CORBA Basics, 2008. http://www.omg.org/gettingstarted/corbafaq.htm

WWW OMNet
Website von OMNeT++, 2008. http://www.omnetpp.org/

WWW OpenDHT
OpenDHT Website, 2008. http://opendht.org/

WWW OverSim
Website von OverSim, 2008. http://www.oversim.org/

WWW P2PRG
Website der IRTF Peer-to-Peer Research Group (P2PRG), 2008. http://www.irtf.org/charter.php?gtype=rg&group=p2prg

WWW P2psip
Website der IETF Working group Peer-to-Peer Session Initiation Protocol (P2PSIP), 2008. http://tools.ietf.org/wg/p2psip/

WWW PPLive
PPLive Website, 2008. http://www.pplive.com/en

WWW Prj Kai
Projekt "Kommunikation mittels Autonomer Infrastrukturen (KAI)", gefördert vom Bundesamt für Sicherheit in der Informationstechnik (BSI), Laufzeit: 2007-2008, 2008. http://dsn.tm.uni-karlsruhe.de/kai-project.php

WWW Prj Sesam
Projekt "Selbstorganisation und Spontaneität in liberalisierten und harmonisierten Märkten (SESAM)", gefördert vom Bundesministerium für Bildung und Forschung (BMBF), Laufzeit: 2003-2007, 2007.
http://www.sesam.uni-karlsruhe.de/

WWW Ron
Website des Projekts Resilient Overlay Networks (RON), 2008.
http://nms.csail.mit.edu/ron/

WWW RTR
Website der österreichischen Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH), 2008. http://www.rtr.at/

WWW save
Website der SavetheInternet.com Coalition, 2008.
http://www.savetheinternet.com/

WWW Sharman
Website von Sharman Networks, Inc., 2008.
http://www.sharmannetworks.com/

WWW Skype
Skype Ltd. Website, 2008. http://www.skype.com/

WWW Skype API
Skype Developer Zone, 2008. https://developer.skype.com/

WWW W3C
Website des World Wide Web Consortium (W3C), 2008. http://www.w3.org/

WWW Wireshark
Wireshark: network protocol analyzer, 2007. http://www.wireshark.org/

Yao et al. 2006
Yao, Z. ; Leonard, D. ; Wang, X. ; Loguinov, D.: Modeling Heterogeneous User Churn and Local Resilience of Unstructured P2P Networks. In: *ICNP '06: Proceedings of the Proceedings of the 2006 IEEE International Conference on Network Protocols*, IEEE Computer Society, 2006. – DOI 10.1109/ICNP.2006.320196. – ISBN 1–4244–0593–9, S. 32–41

Yeager & Bhattacharjee 2005
Yeager, B. ; Bhattacharjee, B.: *IRTF Peer-to-Peer Research Group, Presentation at the 63rd IETF Meeting in Paris 2005*. (WWW-Veröffentlichung). 2005
http://www.cs.umd.edu/projects/p2prg/Paris-2005.ppt

Yu et al. 2008

Yu, H. ; Gibbons, P. ; Kaminsky, M. ; Xiao, F.: SybilLimit: A Near-Optimal Social Network Defense against Sybil Attacks. In: *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, 2008. – DOI 10.1109/SP.2008.13. – ISSN 1081–6011, S. 3–17

Yu et al. 2006

Yu, H. ; Kaminsky, M. ; Gibbons, P. ; Flaxman, A.: SybilGuard: defending against sybil attacks via social networks. In: *SIGCOMM '06: Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications*, ACM, 2006. – DOI 10.1145/1151659.1159945. – ISBN 1–59593–308–5, S. 267–278

Zhang & Lian 2002

Zhang, Z. ; Lian, Q.: Reperasure: Replication Protocol Using Erasure-Code in Peer-to-Peer Storage Network. In: *SRDS '02: Proceedings of the 21st IEEE Symposium on Reliable Distributed Systems (SRDS'02)*, IEEE Computer Society, 2002. – ISBN 0–7695–1659–9, S. 330

Zhao et al. 2004

Zhao, B. ; Huang, L. ; Stribling, J. ; Rhea, S. ; Joseph, A. ; Kubiatowicz, J.: Tapestry: a resilient global-scale overlay for service deployment. In: *Selected Areas in Communications, IEEE Journal on* vol. 22, no. 1 (2004), S. 41–53. – DOI 10.1109/JSAC.2003.818784. – ISSN 0733–8716

Zimmermann 1980

Zimmermann, H.: OSI Reference Model–The ISO Model of Architecture for Open Systems Interconnection. In: *Communications, IEEE Transactions on* vol. 28, no. 4 (1980), S. 425–432. – ISSN 0090–6778

Universität Karlsruhe (TH)
Institut für Telematik

ISBN: 978-3-86644-327-3

www.uvka.de