Beweisbare Privatheitsgarantien durch den Einsatz wiederaufladbarer Energiespeicher

Fabian Laforet, Erik Buchmann, Klemens Böhm

Die globale Energiewende erfordert die Verfügbarkeit von Energieverbrauchsdaten mit einer hohen Auflösung. Intelligente Stromzähler, sogenannte Smart Meter, messen solche Daten in Echtzeit. Dies wiederum gefährdet den Datenschutz: Zeitreihen von Energieverbrauchsdaten enthalten unterschiedliche Arten privater Informationen. So lassen sich neben Tagesabläufen der Bewohner auch Rückschlüsse auf deren Beschäftigungsverhältnis ziehen und sogar die Identifizierung des geschauten Fernsehprogrammes ist möglich. Bedenklich sind solche Informationen beispielsweise, wenn Einbrecher herausfinden können, zu welchen Zeiten niemand zu Hause ist, oder wenn Versicherungen die Daten nutzen, um aufgrund ungesunder Lebensweisen die Beiträge erhöhen. Wir befassen uns mit diesen Problemen, indem wir einen Lösungsansatz [1] zur Störung der Verbräuche vorschlagen, der auf wiederaufladbaren Energiespeichern beruht. Die Energie, die ge- und entladen wird, verrauscht die Daten, die den aktuellen Verbrauch beschreiben. Sogenannte Ladestrategien spezifizieren das Ladeverhalten des Energiespeichers.

Das Hauptziel dieses Beitrages ist es, Privatheitsgarantien für solche Strategien geben zu können. Zu diesem Zweck beruhen die Strategien, die wir vorschlagen, auf einer Verallgemeinerung der Irwin-Hall Verteilung, die Analysen in geschlossener Form ermöglicht. Zunächst betrachten wir den Fall, in dem die Verbräuche mehrerer Haushalte zu Analysezwecken aggregiert werden. Hier können wir (ε, δ)-differential Privacy [2] Garantien geben. Für den Fall, dass die Verbräuche jedes Haushalts individuell vorliegen, schlagen wir ein neues Privatheitsmaß statistischer Natur vor, um das Risiko zu quantifizieren, dass Merkmale zu den Zeitreihen, aus denen heraus sie berechnet wurden, falsch zugewiesen werden. Im Anschluss entwerfen wir eine spezielle Ladestrategie, die die benötigten Eigenschaften, die für die zuvor vorgestellten beweisbaren Privatheitsgarantien notwendig sind, mit einer Trenderhaltung kombiniert, um gegen Filter-Angriff zu schützen. Insgesamt erhöht unsere Strategie die Wahrscheinlichkeit, dass Verfahren fehlschlagen, die private Informationen aus den Daten ableiten [3] [4].

Literaturverzeichnis

[1] Laforet, E. Buchmann und K. Böhm, „Towards Provable Privacy Guarantees Using Rechargeable Energy-Storage Devices," in *ACM e-Energy*, 2016.

[2] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov und M. Naor, „Our Data, Ourselves: Privacy Via Distributed Noise Generation," in *Advances in Cryptology (EUROCRYPT)*, 2006.

[3] C. Beckel, L. Sadamori und S. Santini, „Automatic socio-economic classification of households using electicity consumption data," in *The Fourth International Conference on Future Energy Systems*, 2013.

[4] E. Buchmann, K. Böhm, T. Burghardt und S. Kessler, „Re-identification of Smart Meter data," in *Personal and Ubiquitous Computing*, 2013.