symmetry

MDPI

Review

A Survey of Public Key Infrastructure-Based Security for Mobile Communication Systems

Mohammed Ramadan [1,2,*], Guohong Du [2], Fagen Li [1] and Chunxiang Xu [1]

[1] School of Computer Science and Engineering, University of Electronic Science and Technology of China, Gaoxin West Zone, Chengdu 611731, China; fagenli@uestc.edu.cn (F.L.); chxxu@uestc.edu.cn (C.X.)

[2] School of Electronic Engineering, Chengdu University of Information Technology, Xuefu Road, Chengdu 610225, China; dghong@cuit.edu.cn

* Correspondence: nopatia@gmail.com; Tel.: +86-138-8048-6194

Academic Editor: Young-Sik Jeong

Received: 27 June 2016; Accepted: 18 August 2016; Published: 26 August 2016

Abstract: Mobile communication security techniques are employed to guard the communication between the network entities. Mobile communication cellular systems have become one of the most important communication systems in recent times and are used by millions of people around the world. Since the 1990s, considerable efforts have been taken to improve both the communication and security features of the mobile communications systems. However, these improvements divide the mobile communications field into different generations according to the communication and security techniques such as A3, A5 and A8 algorithms for 2G-GSM cellular system, 3G-authentication and key agreement (AKA), evolved packet system-authentication and key agreement (EPS-AKA), and long term evolution-authentication and key agreement (LTE-AKA) algorithms for 3rd generation partnership project (3GPP) systems. Furthermore, these generations have many vulnerabilities, and huge security work is involved to solve such problems. Some of them are in the field of the public key cryptography (PKC) which requires a high computational cost and more network flexibility to be achieved. As such, the public key infrastructure (PKI) is more compatible with the modern generations due to the superior communications features. This paper surveys the latest proposed works on the security of GSM, CDMA, and LTE cellular systems using PKI. Firstly, we present the security issues for each generation of mobile communication systems, then we study and analyze the latest proposed schemes and give some comparisons. Finally, we introduce some new directions for the future scope. This paper classifies the mobile communication security schemes according to the techniques used for each cellular system and covers some of the PKI-based security techniques such as authentication, key agreement, and privacy preserving.

Keywords: PKI security; mobile communication security; GSM-authentication and key agreement (AKA) security; CDMA-AKA security; long term evolution-authentication and key agreement (LTE-AKA) security

1. Introduction

In recent years, the telecommunication and wired computer communication communities have rapidly developed several mobile technologies. Consequently, different skills and huge efforts are required to counter attacks malicious users particularly on mobile technologies, such as global system for mobile communication (2G-GSM), code division multiple access (3G-CDMA), and long term evolution (4G-LTE) communication systems. This accordingly made mobile security systems a key field that requires great attention and more study. Meanwhile, there is no unique solution to counter the attacks on mobile technologies despite the increasing cooperation between the telecommunication and the Internet industries. For instance, the first Generation 1G mobile telephone systems provided

essentially no security features. The second Generation 2G GSM system was designed such that it provides security similar to that of eavesdropping in fixed phones, and to protect against cloning of mobile identities [1]. Thus, various weaknesses on GSM mobile security systems were revealed by theoretical and practical works (See Section 2.1). The weaknesses found on 2G GSM were taken into account with the emergence of the 3G or CDMA security system. The 3G security system offers new security features and services. In addition, it is important to stress that the 3G security architecture is not to provide a completely secure system, but to build a system that is flexible and adaptable to new challenges [2].

As far as LTE is concerned, despite developed and standardized by the 3GPP and considered the most secure cellular system by providing security enhancements in comparison with GSM and CDMA cellular system, the LTE security architecture still has issues, particularly in key management techniques, such as the lack of privacy-preservation and key forward/backward secrecy. Moreover, most of the existing studies of mobile communication protocols have focused on confidentiality and authentication requirements. The public key infrastructure (PKI) meant that communication entities use two different keys, and was supposedly a good solution for the mobile communication security due to its flexibility and security features. It could be tailored with the new technologies such as 4G and 5G despite their high communication characteristics (Band width, Data rate, etc.) in order to open a new direction for PKI-based security [3].

Motivations

This survey paper took a particular look at the security features that related to authentication and key agreement (AKA) techniques based on PKI, in the field of mobile communication systems, and precisely aims to present a comprehensive review of the most concerning security issues, which are AKA based on PKI security techniques in the mobile communication networks, because they cannot be solved easily by symmetric cryptosystem for some vulnerabilities such as man in the middle attack (international mobile subscriber identity (IMSI) catcher attack) and replay attack. These two attacks are considered to be the most common weaknesses for mobile communication systems. However, this survey paper, in order to be more practical, excluded other security features and requirements such as confidentiality, integrity, privacy, etc. as a priority because most have been covered by symmetric cryptosystems, and this survey only includes the most recent and important works in the security-based PKI for 2G-GSM and 3GPP mobile systems. Moreover, this paper studies and analyzes the existing security solutions using PKI in order to confirm how the previous proposed schemes meet the security requirements, and it suggests some new solutions as well as proposes some new directions and future scopes for compatible and secure cellular systems.

The rest of this paper is organized as follows: Section 2 introduces some background notions on mobile communications security for each cellular generation: 2G-GSM, 3G-CDMA and 4G-LTE respectively. Section 3 discusses the previous work and gives a brief literature review for some of the proposed work in the field of mobile communications security. Section 4 describes the Security requirements and performance analysis for some of the previous work with comparisons. In Section 5, we present security solutions with new directions in the field of PKI-based security for mobile communications. Finally, Section 6 draws some conclusions.

The general architecture for the operation and security processes is shown in Figure 1. There are five operation processes and three security processes in the mobile communications architecture for all the cellular systems, which are shown in (Figure 1) with some clarifications.

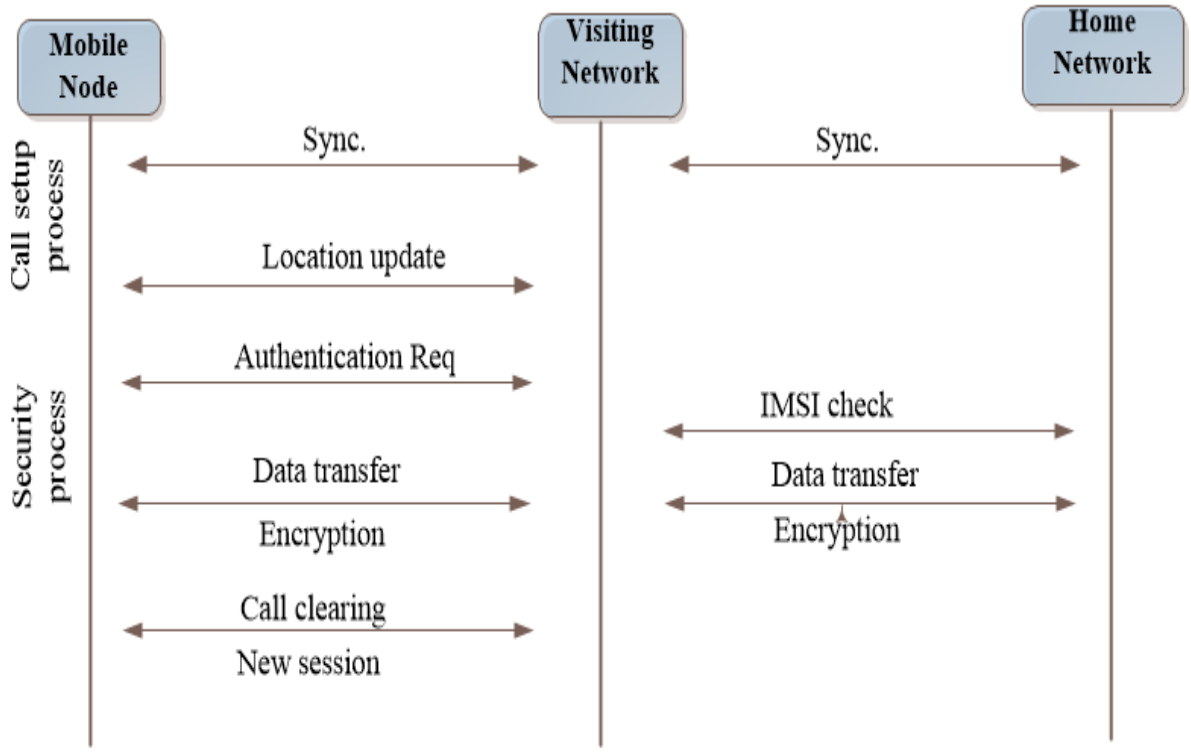

Figure 1. Operation and security processes in mobile architecture.

2. Mobile Communications Security Issues

2.1. 2G-GSM Security

There had been breakthroughs related to the 2G specifications as time went on; many new cryptographic algorithms for GSM, enhanced circuit switched data (ECSD), general packet radio service GPRS, and enhanced data rates for GSM evolution (EDGE) that can be implemented on dual-mode phones were designed in 2002, and finally, A5/3 for GSM and ECSD/EDGE, GEA3 for GPRS, and f8 for universal mobile telecommunication system (UMTS) were proposed, all of them having a similar structure. Considering the network access security, designs were proposed for 2G mobile systems such as GSM and CDMA to counter external attacks, but these designs have led to numerous interception attacks [4–7]. Although the security mechanisms of the GPRS are GSM are similar, GPRS uses the GPRS encryption algorithm (GEA), which currently has three versions: GEA1, GEA2, and GEA3, instead of using the A5 algorithm; In GPRS, the end terminal of encryption is moved towards a deeper point in the network, i.e., the serving GSN (SGSN). It requires the physical layer of the GSM to perform the encryption, and the accomplishment is seen at the logical link control (LLL) layer of the GPRS. Apart from its new offered applications, the UMTS scrutinized the GSM security problems and solved most of them. The main reasons behind GSM security problems were due to the fact that its security was provided by obscurity for the UMTS algorithms to be openly designed; therefore, its algorithms have not faced serious problems. In addition, with the current technology, the theoretical attacks proposed are not practically feasible. Nevertheless, many works proposed to provide security solutions by using PKI techniques.

2.2. 3G-CDMA Security

In 3G network, a radio link of a particular base station (Node B) connects a mobile station to a visited network. Multiple base stations of the network are connected to a Radio Network Controller (RNC) and multiple RNCs are controlled by a GPRS2 support node (GSN) in the packet-switched case

or a mobile switching center (MSC) in the circuit-switched case (see Figure 1). The tracking of all mobile stations that are currently connected to the network are kept by the visitor location register (VLR) and the SGSN, and the identifier of every subscriber, which is permanent, is his IMSI. While the locally valid temporary mobile subscriber identities (TMSI) identifies a subscriber whenever possible, the IMSI is sent over the air interface as frequently as possible in order to protect against profiling attacks. There is a long term secret key Ki shared by both every UMTS subscriber and his dedicated home network. The current location of all subscribers of the home network is tracked by his home location register (HLR). The current SGSN or the MSC/VLR respectively, help carry out the Mutual authentication between a mobile station and a visited network. UMTS supports encryption of the radio interface as well as integrity protection of the signaling messages [8,9]. For a detailed description we refer to [8,9]. Moreover, in order to protect against man-in-the-middle, UMTS-AKA procedure was designed; to protect against network impersonation, UMTS applies both the validity of an authentication token and the integrity protection of the signaling messages. Protecting against replay of authentication data, the freshness and the origin (home network) of the authentication challenge is guaranteed by the authentication token. The integrity protections prevent the possibility that a man-in-the-middle can simply forward correct with timely authentications messages and fool both the mobile station and the base station into not using encryption for subsequent communication [10].

2.3. 4G-LTE Security

Avoiding the weaknesses in the UMTS security mechanism such as man-in-the-middle attacks, rogue base station attacks, and deny of service (DoS) attacks, The LTE security architecture makes better and more attractive the previous generations [11–13]. The expectations from the next generation mobile communication systems are to provide more security functionality than the UMTS systems in order To achieve a mutual authentication between the user equipment (UE) and the mobility management entity (MME) through the evolved-universal terrestrial radio access network (E-UTRAN). The mutual authentication between the UE and the evolved packet core (EPC) is the most important security feature in the LTE security architecture. The AKA procedure is used by the LTE system to achieve the mutual authentication between the UE and the EPC and generate a ciphering key (CK) and an integrity key (IK), that are used to derive different session keys for the encryption and the integrity protection. Several different AKA procedures are implemented in the LTE security architecture when the UEs access to the EPC via distinct access networks because of the support of non-3GPP access [14]. The 3GPP classifies the security architecture of the LTE system into five different functional domains as follows [15].

- **Network access security:** use of universal subscriber identity module (USIM) to provide secure access for a user to the evolved packet system (EPS). Includes mutual authentication and privacy features.
- **Network domain security:** refers to features that allow for secure communications between Evolved Packet System/Evolved Packet Core (EPS/EPC) nodes in order to protect against attacks on the network.
- **User domain security:** securing access to the terminal, e.g., screen lock password, or personal identification number (PIN) to enable USIM usage.
- **Application domain security:** security features used by applications, e.g., hypertext transfer protocol (HTTP).
- **Visibility and configurability of security:** features to allow a user to know whether a security feature is in operation or not, and user-configured control over whether use of a service depends on enabled security features.

3. A Survey of the Literature

Over the last years, there have been many publications aiming to tackle the mobile communications systems security issues. This survey will be divided into two sections depending on each generation, and it includes user's anonymity, privacy preserving, authentication, and key agreement aspects as shown in Figure 2 below:

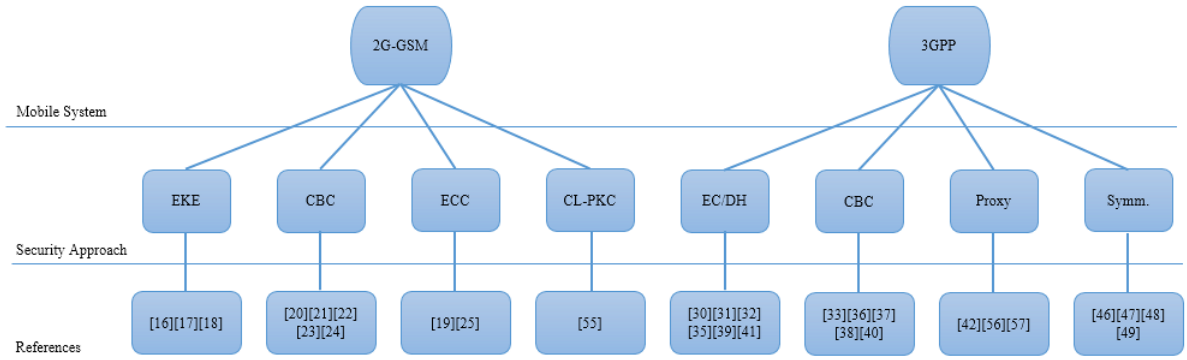

Figure 2. Taxonomy of the PKI-based security approaches in mobile communication systems.

3.1. Review of PKI-Based Security for 2G-GSM Systems

Due to the low communication characteristics of the GSM cellular system, many researchers deployed lightweight cryptosystem algorithms in the field of GSM security, such as elliptic curve cryptosystem (ECC) and Ron Rivest-Adi Shamir-Leonard Adleman algorithm (RSA) algorithm, in order to provide secure authentication between a user and a server using a weak secret, and hence the encrypted key exchange (EKE) protocol is used.

2002 Zhu et al. [16] present a variant of RSA-EKE for mobile devices. In the protocol, the need for per session RSA key generation is cancelled, but an "interactive step" included against e-residue attacks brings additional computational costs on both the server and client sides.

Gong et al [17] follow to propose another influential work on strong user authentication with weak passwords. Gong et al.'s contains a trusted third party which is continuously available online, as in Kerberos. Unlike EKE, there is no need to generate fresh public/private key pairs per session, but there is a need for the trusted server's public key to be known to all parties; in this protocol, by the help of the trusted server, the parties in the system authenticate each other. In order to bring some flexibility to GSM users, Aydemir and Selcuk [18] proposed an authentication protocol for GSM. In this protocol, without interacting with the operator of the service provider by using PINs and passwords, mobile users can redirect their calls, reach their accounts without their subscriber identity module (SIM) card, or easily disable their accounts. All the same, the scheme proposed is not secure since the users can access their accounts without the SIM card, and this mainly eliminates the dependency of the SIM card during authentication.

Ammayappan et al. [19] followed and proposed a GSM authentication protocol using an ECC scheme. This scheme offers better security since it does not use A5/0, A5/1 and A5/2 algorithms, which have been already broken. In addition, this scheme provides mutual authentication, requires less storage, avoids replay attack, consumes smaller network bandwidth, and reduces the storage overhead and bandwidth consumption problem by delegating the key generation operation to the VLR, an advantage indeed. Nevertheless, this scheme provides a new session key for each and every new communication. VLR uses its initial identity for every new communication. The first Phase involves 4 message flows and the second phase involves 2 message flows. This aims to improve some drawbacks of the current GSM authentication protocol, including: not supporting bilateral authentication, huge bandwidth consumption between VLR and HLR, stored space overhead in VLR, and overloaded HLR with authentication of mobile stations.

Lee et al. [20] proposed an extension of the authentication protocol for GSM. In addition, security algorithms A3, A5 and A8 make this new protocol robust. Nevertheless, this scheme provides mutual authentication only for the first time, when the mobile station (MS) joins into the new VLR. Despite this, the scheme proposed a novel authentication protocol which not only clear the drawbacks of the previous works but also make the authentication more efficient. This scheme provide mutual authentication without changes in the basic system architecture, and it's employed that the same encryption algorithms and one-way hash functions used in the basic GSM authentication scheme (A3, A5 and A8). Building on that, each user has its own secret pre-shared key K_0 which is stored in AuC/HLR in advance as well as in SIM/MS. However, in this protocol and for each new communication, VLR computes the certificate to prove its identity even though the MS has stayed in the same VLR. In short, Lee's protocol is based on the idea that AuC/HLR can generate a temporal key that it can be used for the authentication between MSC/VLR and SIM/MS without involving the HLR/AuC in this process, and with zero knowledge of the secret pre-shared key. Therefore, it involves computational overhead, and the same temporary key is reused as long as the MS has stayed in the same VLR. The first and the second phases involve 5 message flows and 2 message flows respectively.

Chang et al. [21] proposed an improvement to Lee et al.'s protocol in [20] such that providing mutual authentication between VLR and MS can be guaranteed all the time while MS sends an authentication request. In addition, this scheme also proposed a relatively new authentication protocol which can not only solve the weaknesses of the pervious works but also make the authentication more efficient. However, in this approach and for each new communication or data session, VLR computes the certificate to verify its identity even though the MS is in the same VLR. Thus, it includes more computational overhead due to the reuse of the same temporary key as long as the MS has remained in the same VLR, and hence the first phase involves 5 message flows and the second phase involves 2 message flows.

Al-Tawil et al. [22] came and proposed an authentication scheme with low handshaking processes and relatively low processing time. This protocol tried to solve the main GSM problems such communication overhead, and computational cost. However, the protocol is lack of mutual authentication property, and it has a high bandwidth consumption and space overhead especially between the network entities.

Lin and Jan [23] followed and proposed an authentication and anonymous channel protocol to be applied over the GSM wireless system without changing the underlying structure. Provided that a PKI exists, Lin and Jan's protocol can be applied over any wireless network. Prepaid tickets perform the anonymity generated by the HLR that can be used later to be authenticated anonymously by VLR. However, the objective of this scheme is to provide complete anonymity, in the sense that nobody (including the HLR) in the system can identify a user who is transmitting over the network. Following Lin and Jan, Alberto [24] proposed an efficient authentication protocol that provides anonymous channels for the GSM system by the means of algorithms A3, A5, A8, and a combination between scheme [22,23]. This protocol covers all the features of Scheme [22] and the anonymity provided in scheme [23], and it is based on the generation of temporal keys defined in [22] the utilization of prepaid tickets [23]. However, the ticket is generated using A3 and A5 algorithms and maintains the general structure of scheme [22].

El Zouka [25] followed and proposed a middleware security system that aims to protect the GSM communication channel. By minimizing the computational overhead of the provided authentication and cryptographic schemes of the network, this scheme provides an end-to-end secured communication between the GSM mobile devices and the GSM base stations; it insures compatibility between wireless GSM devices, and is easy to install without any modification of the basic GSM system. The advantage of this scheme comes from the fact it is based on the ECC and provides as much security as RSA but with less overhead in the processing of messages; therefore, to secretly communicate with each other, mobile terminals must have keys which are known only by the communicating terminals. A random public point, G, is chosen on the elliptic curve (EC), to generate a compressed public key.

3.2. Review of PKI-Based Security for 3GPP Systems

The standard for the 3GPP is evolving the system architecture evolution SAE-LTE architecture for the next generation of mobile communication systems. The SAE/LTE architecture provides secure service as well as 3G wireless local area network (3G-WLAN) interworking [26]. In order to provide secure 3G-WLAN interworking in the SAE/LTE architecture, extensible authentication protocol-authentication and key agreement (EAP-AKA) is used. However, EAP-AKA has several vulnerabilities such as disclosure of user identity, man-in-the middle attacks, sequence number (SQN) synchronization, and additional bandwidth consumption.

The next generation mobile communication system is being developed for secure and fast communication [27]. The SAE/LTE architecture that is being developed by 3GPP provides more secure communication than UMTS [28,29]. To provide mutual authentication between UE and MME through E-UTRAN, the SAE/LTE architecture reuses UMTS-AKA [27]. This AKA protocol is called EPS-AKA. It generates an intermediate key, K-ASME, which can generate 5 keys for protecting transmission between the 3GPP entities [28]. In this section, we present a brief review of the previous works done in the field of AKA for 3GPP networks.

Sandhya et al. [30] proposed a mutual authentication scheme based on secure hash algorithm (SHA) for LTE using hyper elliptic curve cryptography, which is a PKC and helps in secure communication for data exchange. This mutual authentication scheme reduces communication complexity and computation cost by using smaller key sizes, which result in less processing time and also provide security against DoS attacks. Moreover, this scheme offers major advantages over traditional ones such as increased speed, less memory and smaller key sizes with higher level of security.

Gódor and Imre [31] in 2006 proposed an authentication scheme based on PKI for mobile systems (UMTS systems) to solve IMSI issues such as IMSI catcher, and man-in-the-middle (MITM)attack, and provide mutual authentication, integrity, and non-repudiation security requirements. Moreover, in this scheme the IMSI identifier is encrypted on the air interface and use the SQN as a random numbers to protect the users against replay and MITM attacks. However, we clearly can observe that the SQN is used in UMTS for a communication purpose in the particular of multiplexing and multiple access techniques e.g., CDMA as well as in data scrambling technique. Building on that and compared with [21,24] this scheme consider to be impractical with low reliability due to its lack of security parameters functionalities.

On the other hand, Mun et al. [32] studied on the threats and attacks in 3G-WLAN interworking proposed a new AKA protocol based on EAP-AKA, which combines elliptic curve Diffie-Hellman (ECDH) with symmetric key cryptosystem. Furthermore, the proposed protocol provides perfect forward secrecy (PFS), mutual authentication, and resistance to replay attack. Additionally, compared with many previous protocols, which use PKI cryptosystem with certificates, this scheme reduces computational overhead. This is because it does not make SQN synchronization and does not consume bandwidth between the authentication authorization and accounting (AAA) server and the home subscriber server (HSS). Meanwhile, it still has a high computational cost due to the combination of ECDH with symmetric cryptosystems.

Kambourakis et al. [33] proposed techniques for the existing problems that are related to AKA. This include compromising authentication vector attacks as they appear in current 2/2.5G/3G mobile communication systems, the study also proposed a scheme that combined secure sockets layer (SSL) with PKI elements and protects user's identity IMSI. This scheme assumed authentication as a service as to be performed at the higher protocol layers regardless of the basic network technology. Furthermore, the performance measurements are calculated based on "prototype" implementation for handshaking protocols. Their calculations show that SSL-based authentication can be possible in terms of service time in future wireless systems. However, this scheme lacks a roaming-based authentication approach and has relatively high computational cost.

Zheng et al. [34] combined trusted computing (TC) with PKI to provide a significant, robust platform for user access to sensitive service and data in 4G systems. Then, over the trusted mobile platform (TMP), the study also presented a hybrid AKA and authorization scheme, in which the password is combined with a fingerprint as well as a public key to achieve mutual authentication among user i.e., mobile equipment ME/USIM and among user accessed network/home environment (AN/HE). Compared with other AKA for future mobile networks and 3G-AKA, this scheme provides a decent efficiency and relative security to resist potential attacks as well as attacks in heterogeneous network infrastructure. However, this scheme has weaknesses similar to that of [33]. It lacks of internetwork authentication approach and also has relatively high computational cost.

Xu et al. [35] in 2010 reviewed the previous work of Lee et al. [36] and Zhu et al. [37] and claimed that both schemes still suffer from certain weaknesses which have been previously ignored, thus are far from the desired security. Meanwhile, Xu et al. also proposed a mutual authentication and key agreement protocol for roaming services in wireless environments. Similar to [36,37], this work also presented a performance analysis for identity anonymity, key agreement fairness, and user friendliness. Their scheme is assumed to be cost-efficient for a general mobile node (MN). Moreover, this scheme employs a user password and a smart card to preserve the identity anonymity and provides necessary user friendliness. This protocol consists of three phases: out-of-band registration, mutual authentication between the MN and foreign domain, and session key renewal. However, for roaming authentication techniques, the schemes in [35–37] are considered to be more complex due to computational-based operations cost and security parameters exchange.

Haddad et al. [38] proposed a secure authentication of the EPS-AKA for the LTE-A network using PKC for confidentiality and RSA to compute a temporary value to the IMSI, and nonce to generate challenge messages toward the other side. The aim of this work is to solve the problem of sending the IMSI as a clear text, hence preventing the MME attack. Furthermore, the proposed scheme does not need to change the basic framework and the infrastructure of the LTE-AKA network, although a ciphered IMSI is transmitted. The authentication procedure is executed by the HSS to authenticate the UEs and the MME. Therefore, the impersonation of the MME and UEs is unlikely. However, this work is claimed to be secure and able to achieve the security requirements of the LTE-A subscribers such as privacy, authentication, confidentiality and integrity, although it has relatively high communication overhead, and bandwidth consumption.

Abdo et al. [39] defined four security weaknesses in the original LTE AKA protocol: IMSI catching, tracking user temporary identity due to linkability and security network authentication. In addition, the authors proposed two countermeasures to use in order to solve these problems: PKI and pseudonyms based methods. The advantage of this work is the security capabilities that are achieved using the PKI. However, there is a serious problem which has to do with the first hop dependency, where the UE depends on a pre-stored cipher key (CK) and identity key (IK) to generate the initial pseudonyms. CK and IK are generated by the pre-shared cryptographic function using the pre-shared secret key (K) between UE and HSS and a random challenge random number RAND that is generated by the HSS. Therefore, the HSS should be able to perform some calculations before initialization phase, which surely depends on the IMSI.

Abdo et al. [40] proposed a scheme called EPS mutual authentication and Crypt-analyzing (SPAKA), which is a self-certified based protocol, and it solves the positive capturing of the IMSI during user identification and key agreement protocols. The authors use the PKI to encrypt the transmitted AKA messages, and hence it offers a high security level, even though the fake MME is still a problem.

Lai et al. [41] proposed a new scheme for group based communication authentication called a Secure and Efficient group Authentication and key Agreement protocol for LTE networks (SE-AKA) using the ECDH to accomplish the key forward/backward secrecy and also adapt an asymmetric cryptosystem to keep user privacy. For group authentication, SE-AKA uses a group temporary key (GTK), which employs a well-known keys generation algorithm called Diffie-Hellman, and also

provides a strong security level when subscribers need to meet the limitations of the authenticated group before network authentication. However, the problem of this scheme is the consumption of the MME when the ECDH consumes time to generate and exchange the public keys between group members. Meanwhile, the main role of the MME is to work as an access between the HSS and the UEs. In addition, the proposed group is considered as an uncontrolled area in the network and is used to break the security of the network since the authentication approvals are invoked to the group authority instead of the HSS. In addition, the users in group-based communication face new challenges in authentication when they move such as long delay and high computational overhead may take place during handover process.

Jing et al. [42] proposed a privacy preserving handover authentication scheme for EAP based on wireless networks. The authors used the proxy signature scheme to achieve authentication between the MN and the access point (AP) without including the third party. The full security analysis shows that the proposed scheme can accomplish privacy preserving and forward/backward security. The proposed approach is claimed to be more efficient in terms of computation and communication overheads. This work consists of two phases: delegation initialization phase and handover authentication phase. Meanwhile, the proposed scheme can only be deployed in the mobile user side with 2.128 ms, hence has relatively low computational cost compared with the works of Kim et al. [43] and Choi et al. [44].

Kim et al. [43] proposed a handover authentication scheme which uses the ID-based encryption technology to protect the communications in the handover authentication process. However, firstly it needs the private key generator (PKG) to issue the private keys of MNs and APs, which results in the key escrow problem. Secondly, although the PKG updates private keys for MNs and APs every hour, it is possible for adversaries to compromise a private key before the expiration time. As a result, the scheme fails to provide the perfect forward/backward security. Meanwhile, the update of private key every hour cannot perfectly solve the illegal usage of the private key which is revoked before the expiration time. In addition, since it takes two bilinear pairing operations at least on the resource-constrained MNs, this scheme is not efficient in the handover process, as it requires a high computational cost.

Choi et al. [44] proposed a handover scheme using credentials based on chameleon hashing. Actually, the MN and the target AP can achieve mutual authentication and generate the pairwise transient key (PTK) via exchanging their short-term credentials issued by the AAA server. This scheme can achieve the robust key exchange and efficiency in terms of latency performance. Nevertheless, if adversaries compromise the unbroken short-term credentials at any time before expiration, they can calculate the PTKs at any time. Thus, it fails to achieve the perfect forward/backward security. Meanwhile, it does not consider the revocation of short-term credentials. In addition, although MN's real identity is not exposed to adversaries, adversaries can also apply the unbroken short-term credential to trace the movement of MN. Therefore, this scheme failed to achieve privacy preserving.

Cao et al. [45] proposed handover authentication scheme between HeNB and eNB in LTE networks, it is supposed to be fast and secured handover authentication scheme to fit-in with all of the mobility scenarios in the LTE networks. In addition, it is there to provide a number of security features including perfect forward/backward secrecy (PBS/PFS). This scheme consists of two phases: the initial attached phase, which prepares for the next handover authentication, and the uniform handover authentication phase which is for mutual authentication and key agreement between the UE and eNB. The PKI is required to have effect in all of the network entities. It is possible for the network side to support PKI due to processing abilities, and on the user side, the authors observed that it is easy to achieve PKI by the deployment of Trust Environments. Though the proposed scheme has an influence on the current 3GPP standard, it does not use the complex key management methods and also unifies all of mobility scenarios, and this property greatly simplifies the current handover processes, although it is still complicated to achieve and has high computational cost (15.372 ms) compared with the

3GPP-LTE schemes (0.1668 ms). Meanwhile, it is relatively good compared with the cost in the works of Choi et al. [44] which is (18.321 ms).

3.3. Review of Symmetric-Key Based Security for Mobile Systems

Symmetric cryptography (single key cryptography) was the only type of encryption in use before public-key cryptography in 1976. The main idea is to use the same key for encrypt/decrypt or sign/verify unlike PKI cryptosystems which are used different keys. However most of the old security techniques for mobile communication systems based on symmetric cryptosystems due to its low computational cost and communication overhead, but it has low security level than PKI systems. Meanwhile, mobile systems have rapidly developed as well as the PKI techniques which became more flexible and suitable for the recent mobile systems.

In 2009 Chang et al. [46] proposed an efficient authentication scheme with anonymity for global mobility networks (GLOMONET) that uses low-cost functions such as one-way hash functions and exclusive-OR operations. It provides a relatively low computational cost and good resistance against possible attacks such as known-key, forgery, and replay attacks. However, the proposed scheme consists of three phases and three rounds handshaking processes between three entities. Thus, we can note that the proposed scheme has a relatively high exchange processes which is impractical with mobile systems especially in case of roaming. Moreover, the session key is controlled by the mobile user regarding his home agent without including all entities contributions, hence Chang's scheme provide unfair key agreement, besides that the scheme provide no mutual authentication or end-to-end security.

In 2010 He et al. [47] proposed a secure and lightweight authentication scheme with user anonymity for wireless communications. This scheme based on symmetric cryptography, hence it provides a relatively low computational cost. In addition, it requires four message exchanges between mobile user, foreign agent and home agent. The proposed scheme provide session key only between the mobile user and the visited network. In addition, this scheme claimed to provide a smart card security technique only if user password for the smart card remained secure. However, the scheme based on ECC cryptosystems and it used SHA-1 hash function in the authentication phase in total of five phases between four entities and that makes the proposed scheme unsuitable with the mobile systems beside it requires a certificate authority with high handshaking processes cost and does not provide mutual authentication or end-to-end security. In general, Daojing's scheme [47] is not flexible with the requirements of wireless systems.

Gope and Hwang [48] proposed a lightweight mutual authentication and key agreement scheme for GLOMONET providing user anonymity. This scheme tried to correct some of the previous proposed techniques by simplify the scheme especially when we are dealing with lightweight mobile systems. The proposed protocol consists of three phases, and also consists of three entities. However, the proposed scheme lacks of end-to-end security and vulnerable to many kind of attacks. Therefore, in 2016 Gope and Hwang [49] tried to improve their previous scheme and proposed an efficient mutual authentication and key agreement protocol (MAKA) to protect the data flow against interception as well as provide a key agreement technique based on session key. The proposed protocol also consists of three phases: registration, MAKA, and password renewal phase, and consists of three entities: mobile user, foreign agent, and home agent. Though Prosanta's scheme [49] is considered to be a highly secure, provides a relatively low computational cost, and achieves the security requirements, but it still lacks end-to-end security properties even the mobile user can change his/her password without any help from other entities; hence end-to-end security issue is considered as the new challenge for mobile networks today.

To the best of our knowledge, until now there is no authentication scheme for wireless communications based on symmetric key cryptography has been proposed to achieve all the security requirement compared with the proposed PKI-based security schemes, but still are cost-effective solutions. However, from the above analysis we consider the proposed schemes in [48,49] are relatively more secure and efficient protocols, indeed they are more suitable and flexible with mobile systems.

Finally, this review only covered some of many research works that are related to mobile communications security and focus on PKI cryptosystems, in particular the authentication and key agreement approaches, while making reference to the works of many other researchers [50–59] whose research works proposed ways using this approach to improve many problems facing mobile communications security such as replay, IMSI catcher, and false base station (fake MME) attacks. Their research helped provide authentication, key agreement, user anonymity, and privacy to secure network entities from such attacks. Moreover, there are still many other works proposing different methods to protect mobile devices. For instance, Christian et al. [60] proposed a concealment scheme to improve the security of non-protection in mobile operating systems such as iPhone operating system (iOS) devices due to the lack of confidentiality and privacy of these mobile devices [61,62].

4. Security Requirements and Performance Analysis

In this section, we compare schemes in the previous literature to classify which ones satisfy the security requirements for mobile communications systems. (Table 1) demonstrates comparisons of performance efficiency and security requirements for 2G-GSM cellular systems, while (Table 2) demonstrates comparisons of performance efficiency and security requirements for 3GPP cellular systems.

Table 1. Comparison of Performance Efficiency in 2G-GSM Security Schemes.

Reference	Security Technique	Mutual Authentication	Replay Attack	MITM Attack	TTP	End-to-End Security
[16]	RSA-EKE	No	No	No	No	No
[17]	PKI-EKE	No	Yes	No	Yes	No
[18]	PKI-EKE	No	Yes	Yes	Yes	No
[19]	ECC	No	Yes	No	Yes	No
[20]	CBC	Yes	Yes	No	Yes	No
[21]	CBC	Yes	Yes	Yes	Yes	No
[24]	CBC	Yes	Yes	No	No	No
[25]	ECC	No	No	Yes	No	Yes
[55]	CL-PKC	Yes	Yes	Yes	No	Yes

Yes: Robust/Provides No: Not robust/Does not provide.

Table 2. Comparison of performance efficiency in 3GPP security schemes.

Reference	Security Technique	Mutual Authentication	Replay Attack	MITM Attack	TTP	End-to-End Security
[30]	Hyper ECC	Yes	No	Yes	No	Yes
[32]	ECC-DH	Yes	Yes	Yes	No	No
[33]	SSL	No	No	Yes	Yes	No
[34]	CBC-TMP	Yes	Yes	Yes	Yes	No
[35]	DH	Yes	No	Yes	No	No
[36]	CBC	Yes	Yes	No	Yes	No
[37]	CBC	No	Yes	Yes	Yes	No
[38]	RSA	Yes	No	No	Yes	No
[41]	ECC-DH	Yes	Yes	Yes	Yes	No
[42]	Proxy	Yes	No	Yes	No	Yes
[56]	Pairing	Yes	Yes	Yes	Yes	No
[57]	Proxy	Yes	Yes	Yes	No	Yes

Earlier 2G-GSM systems provide low security level A3, A5 and A8 algorithms; for instance, A3 is a challenge-response algorithm that has many weaknesses (See Section 2), especially in cases of mutual authentication, anonymity, IMSI catcher attacks, and replay attacks. However, most of the latest research works try to solve such vulnerabilities by using PKI cryptosystems but still have computational and communication overhead problems i.e., References [21,24,54] provide mutual authentication with relatively high computational cost. On the other hand, References [17,18] have low computational costs without mutual authentication. Other security features, such as End-to-End security which is proposed by Reference [55], can provide a high level of security because there is no need for the trusted third party (TTP), i.e., make the network operator secure by reducing the trust placed on the third party.

In the field of mobile communications and aside from security requirements, the power consumptions, computational cost, and communications overhead are serious issues due to the limitations of mobile

system performance, especially with regard to PKI-based security approaches [63]. The performance evaluation is based on the existing experimental in [64,65] for each of the cryptographic operations by using Multiprecision Integer and Rational Arithmetic C/C++ Library (MIRACLE) [66] in platform with Pentium 4 (PIV) 3 GHZ processor in Windows XP operating system and 512 MB memory. Accordingly, the (relative running time) for the operations employed in the proposed schemes defined in the following terms:

Te: ECC-based scalar multiplication = 0.83 ms
Td: Modular Exponentiation = 1.169 ms
Th: Hash function (e.g., SHA-1, MAC) = 3.04 ms
Tp: Pairing operation = 20.01 ms
Tm: Pairing-based scalar multiplication = 6.38 ms
Ts: Symmetric encryption/decryption (e.g., AES-128) = 0.00541 ms

Other lightweight operations (e.g., exclusive or XOR) = 0.008 µs (Omitted)

Nowadays the processes efficiency has been improved with smart phone. Consequently, 4G and future 5G systems provide no different performance than the current computer. Figure 3 illustrates the comparisons of computational efficiency based on the running time in milliseconds (ms) for each scheme.

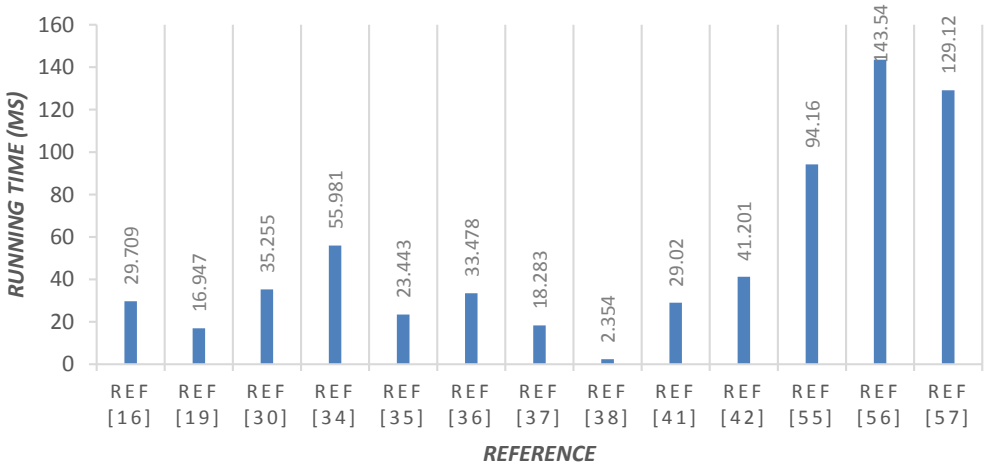

Figure 3. Comparison of computational efficiency.

From the above comparison in (Tables 1 and 3, Figure 3) we found that most of these schemes aim to reduce the computational and communication costs due to the low efficiency of the old cellular systems, with little effort toward achieving basic security requirements. On the other hand, the proposed security schemes in the new cellular systems shown in (Tables 2 and 3, Figure 3) focus on security requirements as well as the computational and communication costs. Building on that, we consider the proposed schemes in References [42,57] are relatively high secure protocols due to their robustness against MITM attacks, in addition to mutual AKA features and independence from trusted third parties. On the other hand, the proposed scheme in References [37,38] are based on PKI cryptosystems, but mobile users only adopted symmetric cryptographic approaches with one-time use of key between mobile user and visited network which leads to low computational cost. However, these schemes and beside the reasonable computational efficiency provide low level of security. For instance, lack of perfect backward secrecy, forgery attack, and mutual authentication property. Nevertheless, the proposed PKI-based approaches suit high performance mobile systems to achieve a desired level of security because mobile networks can never be perfectly secure. The proposed PKI approaches for mobile networks calibrate between computational/communication costs and security requirements, but there are limitations in some aspects.

Table 3. Comparison of computational efficiency in mobile security schemes.

Reference	No. of Phases	Computational Cost	Total Running Time (ms)	Comment
[16]	4	$2Td + 9Th + 2Ts$	29.709	Middle
[19]	3	$4Te + 4Th + 5Ts$	16.947	Low
[30]	4	$4Te + 2Th + 5Td + Tp$	35.255	Middle
[34]	5	$Td + 18Th + 17Ts$	55.981	High
[35]	3	$7Td + 5Th + 11Ts$	23.443	Middle
[36]	3	$11Th + 7Ts$	33.478	Middle
[37]	3	$6Th + 8Ts$	18.283	Low
[38]	4	$2Td + 3Ts$	2.354	Low
[41]	8	$2Te + 9Th$	29.020	Middle
[42]	2	$13Te + 10Th + 2Ts$	41.201	Middle
[55]	4	$2Te + 2Th + Tm + 4Tp$	94.16	High
[56]	6	$9Tm + 2Th + 4Tp$	143.540	High
[57]	3	$5Te + 4Th + 2Tm + 5Tp$	129.120	High

5. New Research Directions and Challenges

In the case of PKI in the field of mobile communications security, we need a flexible network infrastructure, i.e., the service providers are the main candidates to adopt PKI in their systems. Moreover, we need a cellular system with high data rates such as 3GPP systems to be able to implement PKI cryptosystems. The most important entities in PKI systems are a trusted third party and the certification authority to bind the public keys with the corresponding users, as well as the mobile station (mobile equipment and SIM card) that will be responsible for the process of issuing digital certificates. Regarding the importance of secure transactions and the fact that network operators are better candidates for the implementation of a PKI, PKI is expedient to use for transmitting signals within the PLMN, and to secure the entire network. In addition, SIM-card is a new approach that implements personal mobility in addition to terminal mobility. In light of international roaming and support from various services such as telephony, data, fax, and short message service (SMS), the SIM-card is the most important component for security in mobile systems, along with center authentication in the base system. It is especially important if we can improve its efficiency or allow it to improve system security, for example, with the use of new methods of integrated circuits (ICs) and smart card technologies that would make it compatible with the public encryption key.

5.1. Standalone Security System

It is advisable to implement the separation of cellular architecture and security architecture without any communication effects. Thus, to make a complete design, cryptosystems in standalone hardware such as making the authentication center will be a stand-alone entity, and then make the interfaces between them, which makes the system highly reliable security issues, the possibility of development in the future, make sure that the approach is integrated with mobile systems and are compatible with them, and it will be easy to verify system performance.

5.2. Using Secure Algorithms

The service providers can use efficient algorithms such as A5/3 or EPS-AKA, which have been improved to provide a secure system, or can use a newer PKI-based cryptosystem. All these schemes should be implemented on both the network side base transceiver station (BTS) or mobile switching center (MSC/VLR) and the user side (ME or MS/SIM). However, standardization for any modifications in the security or network architectures will require agreement and mutual aid of software and hardware industrialists. In the meantime they should carry out the applicable modifications to their systems. Therefore the cryptosystem should be applied on the mobile stations, and the agreement of mobile phone industrialists is also necessary. Though improvement for the adopted cryptosystems algorithms may not be convenient, if the cryptographic algorithms are substituted with the robust ones,

and the attacker can basically impersonate the real network operator and force the MS/SIM to disable the authentication or the ciphering mode. Hence it is also necessary to modify all security protocols.

5.3. Using End-to-End Security and Reducing Trust on Third Party

The best, easiest, and most profitable solution is to install end-to-end security or security at the application layer. Most mobile communications security vulnerabilities (except SIM cloning and DoS attacks) do not aim at ordinary people. Their targets are usually restricted to special groups so it is reasonable and economical that such groups make their communications secure by using the end-to-end security. Since the encryption and security establishment is performed at the end-entities, changes to the mobile architecture will not be required. In this way, even if the conversation is eavesdropped by the police or legal organizations, they cannot decrypt the transmitted data without having the true CK, provided that a secure enough cryptographic algorithm is deployed. Therefore, in order to avoid illegal activities, it should be transparent to both network operators and service providers. It may also be necessary to find solutions for a legal interception or a key screw scheme. The end-to-end security establishment has complete flexibility with the deployed algorithms so the appropriate upgrades can be easily undertaken when necessary [67].

5.4. Using Lightweight Cryptosystems

Using efficient lightweight schemes such as identity based cryptography (IBC) and certificateless-public key cryptography (CL-PKC) do not require Certificate Authority CA [68]. This leads to lowering the processing time (delay) and handshaking processes. Hence, it can provide more flexibility and security to cellular systems by providing many security goals at once, such as key management, authentication, integrity, confidentiality, privacy preserving, and anonymity. Therefore, we can improve the robustness against attacks: MITM (false base station), IMSI catcher, replay, impersonation, and ensure forward/backward secrecy FBS. Furthermore, this approach has low computational and communication cost with the ability to achieve handover security [69,70].

6. Conclusions

Mobile communications security, having great features, is attractive among users as well as service providers. With the increase in its usage, security problems of confidentiality, integrity, and authentication are also on the rise. The mechanism to solve these problems has changed from symmetric key cryptography to public key cryptography. The available public key cryptographic approaches are good from a security point-of-view but they are computationally extensive and have more signaling overhead. Furthermore, public key cryptography is computationally extensive, and since many sources use it, the current security of mobile communications is not good enough. Therefore, it slows down the data rate. This paper has presented and analyzed some previous works with analysis: some of them are old and in use, while others are under development and standardization. Moreover, we presented some new ideas for the future of mobile communications security using a compatible PKI cryptosystem, especially for privacy preserving, user's anonymity, and AKA security. Hence the suggested new solutions can provide a secure cryptosystem while giving insights into physical security (PHY security) for the mobile communications systems.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Mitchell, C.J. *Security for Mobility*; Institute of Electrical Engineers: London, UK, 2004.
2. *3GPP TS 33.120 (4.0.0), 3G Security: Security Principles and Objectives*; Release 4; 3GPP Organizational Partners: Valbonne, France, 2001.
3. Liang, X.H.; Lu, R.X.; Chen, L.; Lin, X.D.; Shen, X.M. PEC: A privacy preserving emergency call scheme for mobile healthcare social networks. *J. Commun. Netw.* **2011**, *13*, 102–112. [CrossRef]

4. *3GPP TS 21.133, 3GPP: Technical Specification Group Services and System Aspects*; 3G Security; Security Threats and Requirements; 3GPP Organizational Partners: Valbonne, France, 2001.
5. Millan, W. Cryptanalysis of the alleged CAVE algorithm. In Proceedings of the 1st International Conference on Information Security and Cryptology (ICSCI '98), Seoul, Korea, 18–19 December 1998; pp. 107–119.
6. Lauri, P. *GSM Interception*; Lecture Notes; Helsinki University of Technology: Helsinki, Finland, 1999.
7. Wagner, D.; Schneier, B.; Kelsey, J. Cryptanalysis of the cellular message encryption algorithm. In Proceedings of the 17th international conference on cryptology (Crypto'97), Santa Barbara, CA, USA, 17–21 August 1997.
8. *3GPP Technical Specification: 3GPP TS 33.102, V5.3.0, Third Generation Partnership Project; Technical Specifications Group Services and System Aspects; 3G Security; Security Architecture*; 3GPP Organizational Partners: Valbonne, France, 2002.
9. *3GPP Technical Report: 3GPP TR 31.900, V5.3.0. Third Generation Partnership Project; SIM/USIM Internal and External Interworking Aspects; ETSI 3rd Generation Partnership Project (3GPP)*; 3GPP Organizational Partners: Valbonne, France, 2006.
10. *3GPP Technical Specification: 3GPP TS 33.200 version 6.1.0 Release 6, Third Generation Partnership Project; Universal Mobile Telecommunications System (UMTS); 3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security; ETSI 3rd Generation Partnership Project (3GPP)*; 3GPP Organizational Partners: Valbonne, France; March; 2005.
11. Meyer, U.; Wetzel, S. A Man-in-the-Middle Attack on UMTS. In Proceedings of the 3rd ACM Workshop on Wireless Security, Philadelphia, PA, USA, 1 October 2004; pp. 90–97.
12. Zhang, M.; Fang, Y. Security analysis and enhancements of 3GPP authentication and key agreement protocol. *IEEE Trans. Wirel. Commun.* **2005**, *4*, 734–742. [CrossRef]
13. Tang, C.; Wu, D.O. An efficient mobile authentication scheme for wireless networks. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 1408–1416. [CrossRef]
14. *3rd Generation Partnership Project*; Technical Specification Group Service and System Aspects; 3GPP System Architecture Evolution (SAE); Security Architecture (Rel 12) 3GPP TS 33.401 V12.5.0; 3GPP Organizational Partners: Valbonne, France, 2012.
15. *3GPP EPS/EPC Security Architecture*; 3GPP TS 33.401, System Architecture Evolution (SAE)-Security architecture EPS (EPC and E-UTRAN) Security Architecture; 3GPP Organizational Partners: Valbonne, France, 2008.
16. Zhu, F.; Wong, D.S.; Chan, A.H.; Ye, R. Password authenticated key exchange based on RSA for imbalanced wireless networks. In Proceedings of the 5th International Conference on Information Security, London, UK, 12–13 September 2002; Springer-Verlag: Berlin/Heidelberg, Germany, 2002; pp. 150–161.
17. Gong, L.; Lomas, T.M.A.; Needham, R.M.; Saltzer, J.H. Protecting poorly chosen secrets from guessing attacks. *IEEE J. Sel. Areas Commun.* **1993**, *11*, 648–656. [CrossRef]
18. Aydemir, O.; Selcuk, A.A. A strong user authentication protocol for GSM. In Proceedings of the 14th IEEE International Workshop on Enabling Technologies Infrastructure for Collaborative Enterprise (WETICE'05), Linkopings, Sweden, 13–15 June 2005.
19. Ammayappan, K.; Saxena, A.; Negi, A. Mutual authentication and key agreement based on elliptic curve cryptography for GSM. In Proceedings of the 14th International Conference on Advanced Computing and Communications (ADCOM), Mangalore, India, 20–23 December 2006; pp. 183–186.
20. Lee, C.C.; Hwang, M.S.; Yang, W.P. Extension of authentication protocol for GSM. *IEE Proc. Commun.* **2003**, *150*, 91–95. [CrossRef]
21. Chang, C.C.; Lee, J.S.; Chang, Y.F. Efficient authentication protocols of GSM. *Comput. Commun.* **2005**, *28*, 921–928. [CrossRef]
22. Al-Tawil, K.; Akram, A.; Youssef, H. A new authentication protocol for GSM networks. In Proceedings of the IEEE 23rd Annual Conference on Local Computer Networks (LCN'98), Washington, DC, USA, 11–14 October 1998; pp. 21–30.
23. Lin, W.D.; Jan, J.K. A wireless-based authentication and anonymous channels for large scale area. In Proceedings of the Sixth IEEE Symposium on Computers and Communications (ISCC'01), Hammamet, Tunisia, 3–5 July 2001; pp. 36–41.
24. Alberto, P. Privacy and authentication protocol providing anonymous channels in GSM. *Comput. Commun.* **2004**, *27*, 1709–1715.
25. El Zouka, H.A. Providing end-to-end secure communicationsin gsm networks. *Int. J. Netw. Secur. Its Appl. IJNSA* **2015**, *7*. [CrossRef]

26. Lescuyer, P.; Lucidarme, T. *Evolved Packet System (EPS): The LTE and SAE Evolution of 3G*; John Wiley & Sons: New York, NY, USA, 2008.
27. *Third Generation Partnership Project (3GPP), 3GPP TS 33.102 v8.0.0. 3G Security: Security Architecture*; Release 8; 3GPP Organizational Partners: Valbonne, France, 2008.
28. *Third Generation Partnership Project (3GPP), 3GPP TS 33.401 v8.1.1 3G System Architecture Evolution (SAE): Security Architecture*; Release 8; 3GPP Organizational Partners: Valbonne, France, 2008.
29. *Third Generation Partnership Project (3GPP), 3GPP TS 33.821 v1.0.0. Rationale and Track of Security Decisions in Long Term Evolved (LTE) RAN/3GPP System Architecture Evolution (SAE)*; Release 8; 3GPP Organizational Partners: Valbonne, France, 2007.
30. Sandhya, P.; Poovizhi, S.; Varun, R. SHA-based mutual authentication in long term evolution using hyper elliptic curve cryptography. *Int. J. Emerg. Sci. Eng. (IJESE)* **2013**, *1*, 54–55.
31. Gódor, G.; Imre, S. Novel authentication algorithm-public key based cryptography in mobile phone systems. *IJCSNS Int. J. Comput. Sci. Netw. Secur.* **2006**, *6*, 126–134.
32. Mun, H.; Han, K.; Kim, K. 3G-WLAN Interworking: Security analysis and new authentication and key agreement based on EAP-AKA. In Proceedings of the IEEE Wireless Telecommunications Symposium WTS, Prague, Czech Republic, 22–24 April 2009; pp. 1–8.
33. Kambourakis, G.; Rouskas, A.; Gritzalis, S. Performance evaluation of public key-based authentication in future mobile communication systems. *EURASIP J. Wirel. Commun. Netw.* **2004**, *1*, 184–197. [CrossRef]
34. Zheng, Y.; He, D.; Tang, X.; Wang, H. AKA and authorization scheme for 4G mobile networks based on trusted mobile platform. In Proceedings of the 2005 Fifth International Conference on Information, Communications and Signal Processing, Bangkok, Thailand, 6–9 December 2005; pp. 976–980.
35. Xu, J.; Zhu, W.; Feng, D. An efficient mutual authentication and key agreement protocol preserving user anonymity in mobile networks. *Comput. Commun.* **2011**, *34*, 319–325. [CrossRef]
36. Lee, C.C.; Hwang, M.S. Security enhancement on a new authentication scheme with anonymity for wireless environments. *IEEE Trans. Indus. Electron.* **2006**, *53*, 1683–1686. [CrossRef]
37. Zhu, J.; Ma, J. A new authentication scheme with anonymity for wireless environments. *IEEE Trans. Consum. Electron.* **2004**, *50*, 230–234.
38. Haddad, Z.J.; Taha, S.; Ismail, I.A.S. SEPS-AKA: A secure evolved packet system authentication and key agreement scheme for LTE-A networks. *Comput. Sci. Inf. Technol.* **2014**, *58*, 57–70.
39. Abdo, J.B.; Demerjian, J.; Chaouchi, H.; Pujolle, G. EC-AKA2 a revolutionary aka protocol. In Proceedings of the 2013 International Conference on Computer Applications Technology (ICCAT), Sousse, Tunisia, 20–22 January 2013; pp. 1–6.
40. Abdo, J.B.; Demerjian, J.; Ahmad, K.; Chaouchi, H.; Pujolle, G. EPS mutual authentication and crypt-analyzing SP-AKA. In Proceedings of the 2013 International Conference on Computing, Management and Telecommunications (ComManTel), Ho Chi Minh City, Vietnam, 21–24 January 2013; pp. 303–308.
41. Lai, C.; Li, H.; Lu, R.; Shen, X.S. SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks. *Comput. Netw.* **2013**, *57*, 3492–3510. [CrossRef]
42. Jing, Q.; Zhang, Y.; Fu, A.; Liu, X. A privacy preserving handover authentication scheme for EAP-based wireless networks. In Proceedings of the 2011 IEEE Global Telecommunications Conference (GLOBECOM 2011), Houston, TX, USA, 5–9 December 2011; pp. 1–6.
43. Kim, Y.; Ren, W.; Jo, J.; Yang, M.; Jiang, Y.; Zheng, J. SFRIC: A secure Fast roaming scheme in wireless LAN using ID-based cryptography. In Proceedings of the 2007 IEEE International Conference on Communications ICC, Glasgow, Scotland, 24–28 June 2007; pp. 1570–1575.
44. Choi, J.; Jung, S. A Handover authentication using credentials based on chameleon hashing. *IEEE Commun. Lett.* **2010**, *14*, 54–56. [CrossRef]
45. Cao, J.; Li, H.; Ma, M.; Zhang, Y.; Lai, C. A simple and robust handover authentication between HeNB and eNB in LTE networks. *Comput. Netw.* **2012**, *56*, 2119–2131. [CrossRef]
46. Chang, C.C.; Lee, C.Y.; Chiu, Y.C. Enhance authentication scheme with anonymity for roaming service in global mobility networks. *Comput. Commun.* **2009**, *32*, 611–618. [CrossRef]
47. He, D.; Ma, M.; Zhang, Y.; Chen, C. A strong user authentication scheme with smart cards for wireless communications. *Comput. Commun.* **2011**, *34*, 367–374. [CrossRef]
48. Gope, P.; Hwang, T. Lightweight and energy efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks. *IEEE Syst. J.* **2015**. [CrossRef]

49. Gope, P.; Hwang, T. An efficient mutual authentication and key agreement scheme preserving strong anonymity of the mobile user in global mobility networks. *J. Netw. Comput. Appl.* **2016**, *62*, 1–8. [CrossRef]
50. Zhang, Y.; Chen, X.; Li, J.; Li, H. Generic construction for secure and efficient handoff authentication schemes in EAP-based wireless networks. *Comput. Netw.* **2014**, *75*, 192–211. [CrossRef]
51. Huang, Y.; Shen, C.; Shieh, S.W. S-AKA: A provable and secure authentication key agreement protocol for UMTS networks. *IEEE Trans. Veh. Technol.* **2011**, *60*, 4509–4519. [CrossRef]
52. Park, C. Authentication protocol providing user anonymity and untraceability in wireless mobile communication systems. *Comput. Netw.* **2004**, *44*, 319–333. [CrossRef]
53. Palekar, A.; Simon, D.; Josefsson, S.; Zhou, H.; Zorn, G. Protected EAP Protocol (PEAP) Version 2, IETF, October 2004. Available online: https://www.ietf.org/archive/id/draft-josefsson-pppext-eap-tls-eap-10.txt (accessed on 24 August 2016).
54. Han, L. *A Threat Analysis of the Extensible Authentication Protocol*; Honors Project Report; Carleton University: Ottawa, ON, Canada, 2006.
55. Ramadan, M.; Li, F.; Xu, C.X.; Abdalla, A.; Abdalla, H. An efficient end-to-end mutual authentication scheme for 2G-GSM system. In Proceedings of the 2016 IEEE International Conference on Big Data Analysis (ICBDA 2016), Hangzhou, China, 12–14 March 2016; pp. 1–6.
56. Ramadan, M.; Li, F.; Xu, C.X.; Oteng, K.; Ibrahim, H. Authentication and key agreement scheme for CDMA cellular system. In Proceedings of the 2015 IEEE International Conference on Communication Software and Networks (ICCSN), Chengdu, China, 6–7 June 2015; pp. 118–124.
57. Ramadan, M.; Li, F.; Xu, C.X.; Mohamed, A.; Abdalla, H.; Abdalla, A. User-to-user mutual authentication and key agreement scheme for LTE cellular system. *Int. J. Netw. Secur.* **2016**, *18*, 769–781.
58. D'Orazio, C.J.; Choo, K.R.; Yang, L.T. Data exfiltration from internet of things devices: iOS devices as case studies. *IEEE Internet Things J.* **2016**. [CrossRef]
59. Hwang, T.; Gope, P. Provably secure mutual authentication and key exchange scheme for expeditious mobile communication through synchronously one-time secrets. *Wirel. Pers. Commun.* **2014**, *77*, 197–224. [CrossRef]
60. D'Orazio, C.; Ariffin, A.; Choo, K.R. iOS anti-forensics: How can we securely conceal, delete and insert data? In Proceedings of the 2014 47th Hawaii International Conference on System Science, Waikoloa, HI, USA, 6–9 January 2014.
61. Do, Q.; Martini, B.; Choo, K.R. Is the data on your wearable device secure? An android wear smartwatch case study. In *Software: Practice and Experience (Softw. Pract. Exper.)*; Wiley Online Library: New York, NY, USA, 2016.
62. Do, Q.; Martini, B.; Choo, K.R. A forensically sound adversary model for mobile devices. *PLoS ONE* **2015**, *10*, e0138449. [CrossRef] [PubMed]
63. Azfar, A.; Choo, K.R.; Liu, L. Android mobile VoIP apps: A survey and examination of their security and privacy. *Electron. Commer. Res.* **2016**, *16*, 73–111. [CrossRef]
64. He, D.; Chen, J. An efficient certificate-less designated verifier signature scheme. *Int. Arab J. Inf. Technol.* **2013**, *10*, 389–396.
65. Hea, D.; Chen, J.; Zhang, R. An efficient identity-based blind signature scheme without bilinear pairings. *Comput. Electr. Eng.* **2011**, *37*, 444–450. [CrossRef]
66. Scott, M. *MIRACLE-Multiprecision Integer and Rational Arithmetic C/C++ Library*; Shamus Software Ltd.: Dublin, Ireland, 2003.
67. Ramadan, M.; Du, G.; Li, F.; Xu, C.X. EEE-GSM: End-to-End Encryption Scheme over GSM System. *Int. J. Secur. Appl.* **2016**, *10*, 229–240, ISSN:1738-9976 IJSIA. [CrossRef]
68. Al-Riyami, S.; Paterson, G. Certificateless public key cryptography. In *Advances in Cryptology-ASIACRYPT*; Springer: Berlin/Heidelberg, Germany, 2003; pp. 452–473.
69. Lee, S.; Kim, Y.; Han, J.; Lee, D. Protection method for data communication between ADS-B sensor and next-generation air traffic control systems. *Information* **2014**, *5*, 622–633. [CrossRef]
70. Yang, C.; Sun, Y.; Wu, Q. Batch attribute-based encryption for secure clouds. *Information* **2015**, *6*, 704–718. [CrossRef]