Security Management in the Next Generation Wireless Networks

Yan Zhang and Masayuki Fujise
(Corresponding author: Yan Zhang)

Wireless Communications Laboratory, NICT Singapore
National Institute of Information and Communications Technology (NICT), Singapore 117674
Email: (yanzhang@ieee.org and fujise@nict.go.jp)

(Invited Paper)

Abstract

In this paper, we make an introduction to the security management in the next generation wireless mobile networks, including the access security mechanisms in the circuited-switched domain, packet-switched domain and emerging IP multimedia subsystem domain. Several research challenges are identified, including security architecture with network heterogeneity, energy-security tradeoffs and mobility-security interaction. The identified issues can serve as the potential guidance for further study to satisfy higher security requirement and lower introduced overhead.

Keywords: Access security, confidentiality, energy management, IMS, integrity, mobility management, security management, UMTS

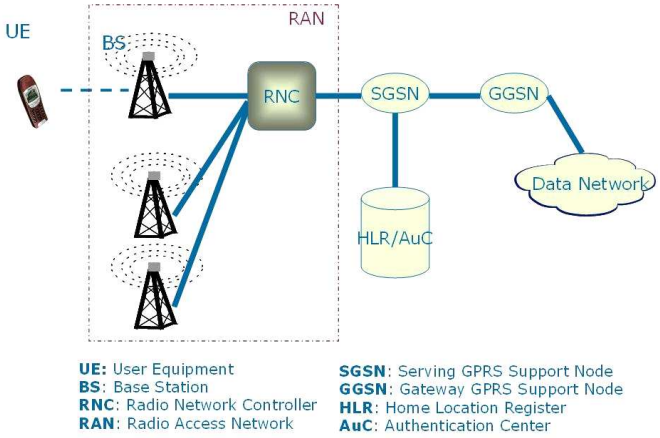


Figure 1: UMTS network architecture

1 Introduction

Universal Mobile Telecommunications System (UMTS) is the natural successor of the current extremely popular Global System for Mobile Communications (GSM) [15]. Code Division Multiple Access 2000 (CDMA2000) is the next generation version for the CDMA-95, which is predominantly deployed in the North America and North Korea. TD- SCDMA is in the framework of 3GPP2 and is expected to be one of the principle technologies employed in China [13, 15]. It is envisioned that each of three standards in the framework of International Mobile Telecommunications-2000 (IMT-2000) will play a significant role in the future due to the backward compatibility, investment and even politics. In all of the potential standards, security management is one of the primary demands as well as challenges to resolve the deficiency existing in the second generation wireless mobile networks such as GSM, where only one-way authentication is performed for the core network part to verify the User Equipment (UE) [3].

Figure 1 shows the UMTS network architecture [2, 4]. UE utilizes the circuited-switched or packet-switched service through the radio interface between Base Station (BS) and itself. Radio Network Controller (RNC) supervises the activities of several BS under its management. Radio Access Network (RAN) consists of the RNC and the according BS. Home Location Register (HLR) stores the permanent information for the subscribers, e.g. International mobile subscriber identity (IMSI), subscribed service profile, identity of current location area. Authentication Center (AuC) is responsible to verify the validness of user's activity including call behavior and location management. Serving GPRS support node (SGSN) connects the core network and the radio access network, and is responsible for location management and for delivering packets between UE and the core network. Gateway GPRS support node (GGSN) acts similarly as a gateway between core network and the external IP networks such as Internet and enterprise Intranets.

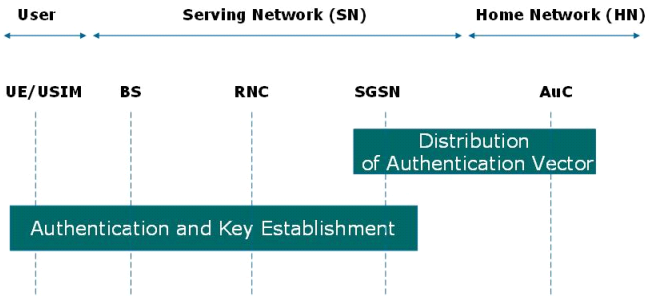


Figure 2: UMTS network Authentication and Key Agreement (AKA)

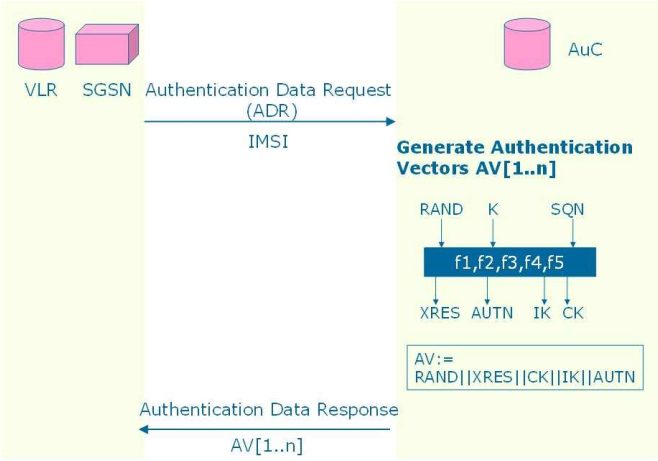


Figure 3: AKA phase 1 – Distribution of authentication vector

2 Access Security

Figure 2 shows the most important feature in the framework of UMTS security management, i.e. Authentication and Key Agreement (AKA) [3]. Authentication refers to the mutual authentication mechanism that the subscriber is able to authenticate the network, and the network is also able to authenticate the user. Key agreement refers to the mechanism to generate the cipher key and integrity key. The events for triggering the AKA process include location update request, user registration, service request, attach request, detach request and connection re-establishment request. The authentication protocol is based on a permanent secret key **K** (128-bit) that is shared between the UE and HLR/AuC. The AKA mechanism can be divided into two phases: the Distribution of Authentication Vector (AV) from the HLR/AuC to the SGSN as shown in Figure 3, and the Authentication and Key Establishment between the UE and the core network as illustrated in Figure 4.

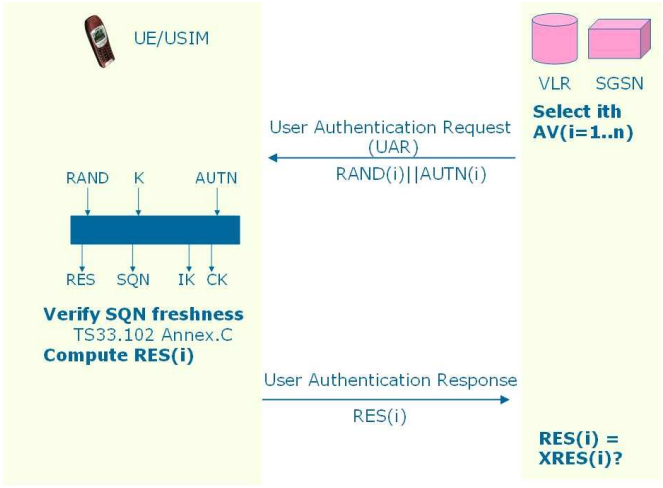


Figure 4: AKA phase 2 – Authentication and key establishment

2.1 Distribution of Authentication Vector

When an UE leaves an old SGSN (SGSNo) and moves into the coverage of a new SGSN (SGSNn), SGSNn has no corresponding record for the UE, which makes it necessary to authenticate the UE prior to the subsequent behavior. SGSNn will delivery an Authentication Data Request (ADR) to the HLR/AuC with the UE's unique IMSI. Based on the received IMSI, AuC can find the associated record and hence the according master key **K** for the particular UE. Then, HLR/AuC generates number of **n** Authentication Vector (AV) instead of single one AV for the sake of saving signaling overhead. The AV structure is comprised of five components: a random number **RAND**, an expected authentication response **XRES**, a cipher key **CK**, an integrity key **IK** and a network authentication token **AUTN** [10]. In each generation, an AV is calculated by means of the authentication function f1-f5, where for instance f1 is employed to compute XRES [11, 12, 13]. After successfully generating **n** AVs, AuC sends back the AV array to SGSNn via the message Authentication Data Response, and SGSNn saves the **n** AVs for the particular UE. It is noteworthy that this phase executes not only upon UE entering a new SGSN area, but also when there are no AVs available upon an action arrival which requires authentication.

2.2 Authentication and Key Establishment

For each activity triggering authentication request such as call origination, paging or location update, the SGSN initiates the challenge User Authentication Request (UAR) message to the UE with the parameters **RAND** and **AUTN**, which is retrieved from the ith ($i = 1, 2, \cdots, n$) AV in the First-in-first-out(FIFO) manner. Upon receiv-

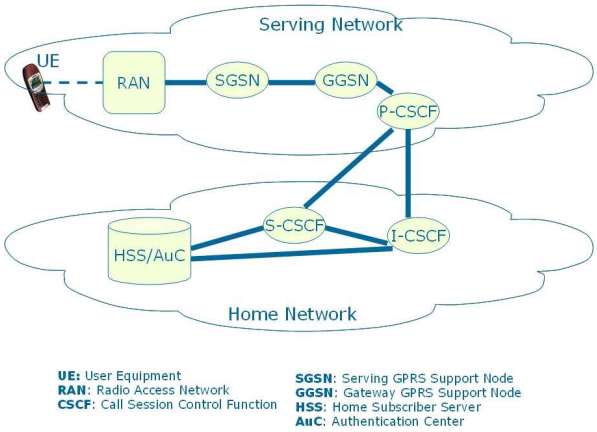


Figure 5: IMS network architecture

ing the AV, the UE checks the validity of **AUTN**. For this goal, the UE retrieves SQN component from **AUTN** and calculates XMAC-A. The UE then compares X-MAC-A and MAC-A component in **AUTN**, if they are equal to each other, then the network is verified. Otherwise, the UE rejects the UAR and hence the network. After the network is identified, UE checks the SQN freshness, i.e. the SQN has never been used before. When succeeds, the UE then computes the authentication response **RES** from the received **RAND** value and sends it in a User Authentication Response message to the SGSN. If **RES** equals the expected response **XRES**, then the UE is successfully authenticated.

It is believed that, after the AKA procedure, all messages are claimed integrity protection, and the signaling data as well as user data are confidentiality protection. In the sense of integrity protection, the content of signaling messages should not be manipulated. With regard to confidentiality protection, the subscriber identification, location, user data and signaling data should be encrypted.

3 Security in IP Multimedia Subsystem (IMS)

3.1 Security Features

Multimedia service provisioning is one of the primary demands and motivations for the next generation wireless networks. To achieve this goal, the IP multimedia subsystem (IMS) is added as the core network in UMTS providing the multimedia service, e.g. voice telephony, video conference, real-time streaming media, interactive game, and instant messaging [9]. The multimedia session management, initialization and termination are specified and implemented in the Session Initiation Protocol (SIP) [7, 19]. There are three entities relevant to the IMS security architecture (See Figure 5). A proxy call session control function (P-CSCF) locates in the serving network of an UE and acts as the first access point in the serving network. P-CSCF is responsible for forwarding SIP messages of an UE to the home network. A serving call session control (S-CSCF) locates in the home network to provide session control of multimedia services and acts as SIP registrar or SIP proxy server. The S-CSCF sends messages toward the Home Subscriber Server (HSS) and the AuC to receive subscriber data and authentication information. An interrogating call session control function (I-CSCF) locates in the home network and acts as a SIP proxy toward the home network. I-CSCF is responsible for selecting an appropriate S-CSCF for the UE, and forwarding SIP requests/responses toward the S-CSCF.

Different from the one-pass authentication procedure in AKA illustrated in Figure 2, the security in IMS is a two-pass authentication procedure, including GPRS authentication and IMS authentication [8]. Before utilizing the IMS service, an UE should first setup a data connection to know the IP address of P-CSCF and to carry the SIP signaling messages through the P-CSCF. The data connection establishment is comprised of two steps, i.e. Attach and Packet Data Protocol (PDP) Context Activation. The first phase Attach is used to establish mobility management context between the UE and SGSN. During this procedure, the UE should perform GPRS authentication and GPRS registration to verify its validness and retrieve the subscriber profile including subscribed services, QoS profile, IP address and so on. Once the UE is attached, the second step PDP context activation is followed to activate a PDP address and build the association between the SGSN and GGSN. Only after attached and PDP context activation, an UE can access IMS services through registration process. The registration is necessary to inform the HSS the location, authenticate and download subscriber profile to S-CSCF. Since this paper concentrates on the security issues, we will discuss the GPRS authentication and IMS authentication in the following two subsections. The discussion of either GPRS registration or PDP context activation is out of the scope and the readers are suggested to refer to the related technical specifications [4].

3.2 GPRS Authentication

GPRS authentication is performed in the framework of GPRS mobility management (GMM) [1, 4]. Figure 6 shows the messages sequence in GPRS authentication. In particular, the steps include

1) The UE sends **GMM Attach Request (IMSI)** to the SGSN with the unique identity **IMSI**.

2) If the SGSN has at least one AV for the UE, then the following Step 2) and 3) are skipped. Otherwise, the SGSN has to obtain AVs from the entity HSS/AuC. SGSN triggers the *procedure Distribution of Authentication Vector* by sending a **MAP-SEND-AUTHENTICATION-INFO Request (IMSI)** message to the HLR/AuC with the parameter **IMSI** uniquely identifying the UE.

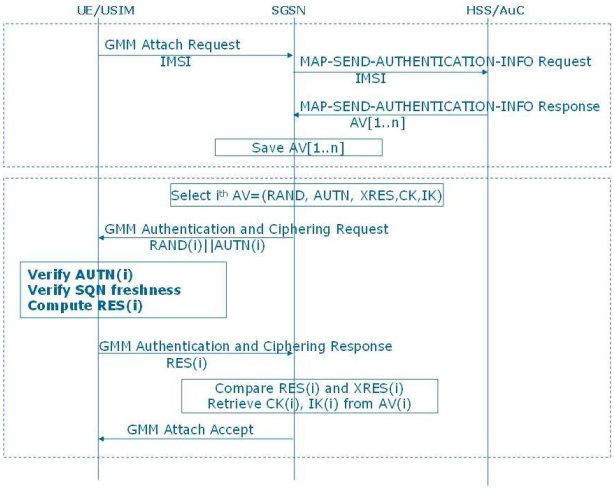


Figure 6: GPRS authentication

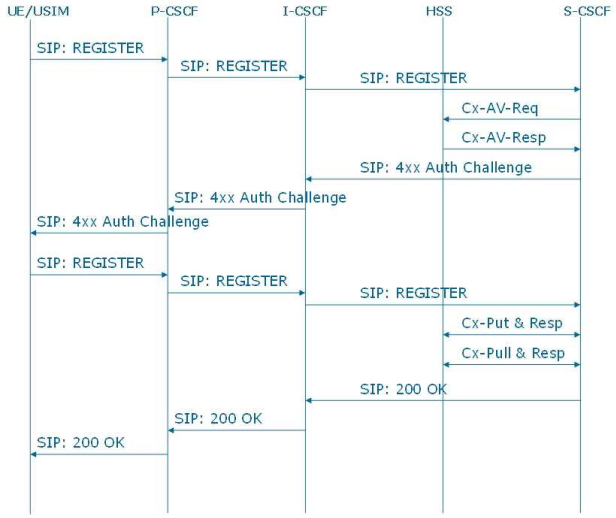


Figure 7: IMS authentication

3) Upon receiving the authentication request, the HSS/AuC searches the according record in the database on the basis of **IMSI**. Then, HSS/AuC generates an ordered array of **n** AVs for the specific UE. Each AV consists of the following components: a random number **RAND**, an expected response **XRES**, a cipher key **CK**, an integrity key **IK** and an authentication token **AUTN**. The HSS/AuC then sends back the message **MAP-SEND-AUTHENTICATION-INFO Response** to SGSN with the AV array as parameters.

4) SGSN stores these n AVs for the particular UE and shall choose the next unused AV in the ordered AV array. Subsequently, the SGSN shall challenge the UE and sends message **GMM Authentication and Ciphering Request** with parameters **RAND** and **AUTN** populated from the selected AV.

5) The UE checks the validness of the received **AUTN**. In case it is acceptable, the UE shall calculate a response **RES** and send back to the SGSN through the message **GMM Authentication and Ciphering Response**. The SGSN retrieves the expected response **XRES** from the selected AV, and compares **XRES** with the received response **RES**. If they match, the authentication and key agreement is successfully completed and the keys **CK** and **IK** are retrieved for the following signaling confidentiality and integrity protection.

6) The SGSN sends a **GMM Attach Accept** message to the UE to indicate the completion of the successful attach procedure.

3.3 IMS Authentication

After the procedures of GPRS authentication, GPRS registration and PDP context activation, the UE has the IP address of the P-CSCF and is able to access the IMS services through the registration procedure using SIP and Cx commands as shown in Figure 7 [5, 6]. This procedure includes the IMS authentication and the IMS registration. In particular, the steps include

1) To start registration, the UE sends a **SIP REGISTER (IMPI, IMPU)** message to the P-CSCF in the serving network. On the receipt, the P-CSCF forwards the registration request to the I-CSCF of the home network. I-CSCF then delivery the message to a chosen S-CSCF.

2) If the S-CSCF has at least one AV for the UE, then Step 2) and 3) are skipped. Otherwise, the S-CSCF has to obtain AVs from the entity HSS/AuC. S-CSCF triggers the procedure *Distribution of Authentication Vector* by sending a **Cx-AV-Req(IMPI, n)** message to the HSS/AuC with the parameter **IMPI** uniquely identifying the UE and the number of **n** AVs wanted.

3) Upon receipt of a request from the S-CSCF, the HSS/AuC searches the database on the basis of the unique **IMPI**, obtains the subscriber profile, and generates an ordered array of **n** AVs for the specific UE. Each AV consists of the following components: a random number **RAND**, an expected response **XRES**, a cipher key **CK**, an integrity key **IK** and an authentication token **AUTN**. Each AV is good for only one authentication and key agreement between the IMS subscriber and the S-CSCF. The HSS/AuC then sends back the message **Cx-AV-Req-Resp(IMPI, RAND1||AUTN1||XRES1||CK1||IK1,..., RANDn||AUTNn||XRESn||CKn||IKn)** to the S-CSCF with the array of AV as parameters.

4) The S-CSCF chooses the first unused AV in the array

of AVs based on FIFO policy. From the selected AV, the items **RAND, AUTN, IK** and **CK** are populated. The S-CSCF sends the message **SIP 4xx-Auth-Challenge (IMPI, RAND, AUTN, IK, CK)** to the I-CSCF, which then forwards the message to P-CSCF. Upon the receipt, the P-CSCF shall store the two keys **IK** and **CK** and remove the key information and finally forward the rest of the message **SIP 4xx-Auth-Challenge (IMPI, RAND, AUTN)** to the UE.

5) The UE verifies the freshness of the received **AUTN** and calculates a response **RES**. This result **RES** is sent back from the UE to the P-CSCF through the message **SIP REGISTER (IMPI, RES)**. After receiving the request, the P-CSCF forwards it to the I-CSCF, which further forwards the authentication response to the S-CSCF. The S-CSCF retrieves the expected response **XRES**, and compares **XRES** and the received response **RES**. If they match, the authentication and key agreement is successfully completed. Next three steps perform registration.

6) The S-CSCF sends a **Cx-Put** message to the HSS/AuC with the UE identity. The HSS shall store the S-CSCF name which is presently serving the UE and then sends the **Cx-Put Response** for acknowledgement.

7) Next, the S-CSCF sends a **Cx-Pull** to the HSS/AuC with the UE identity in order to download the related information in the subscriber profile to the S-CSCF. HSS shall send a **Cx-Pull Response** to the S-CSCF with the indicated information.

8) The S-CSCF sends **SIP 200 OK** message to the UE through the I-CSCF and P-CSCF. After this step, a security associate (SA) is active for the protection of subsequent SIP messages between the UE and the P-CSCF.

4 Research Challenges

4.1 Security Management in Heterogeneous Networks

The next generation wireless mobile networks are characterized by the co-existent of the variety of network architectures due to the diverse requirements for data rate, radio coverage, deployment cost and multimedia service. The 3GPP is actively specifying the roaming mechanism in the integrated Wireless LAN/UMTS networks. It should be noted that this scenario is only a specific heterogeneous network. The IEEE 802.16 standard is an emerging broadband wireless access system specified for wireless Metropolitan Area Networks (Wireless MAN) bridging the last mile, replacing costly wireline and also providing high speed multimedia services. The recently amendment 802.16e adds mobility component for Wireless MAN and defines both physical and MAC layers for combined fixed and mobile operations in licensed bands. It is envisaged that the future generation wireless networks is the flexible and seamless integration of the three technologies Wireless LAN, Wireless MAN and Wireless Wide Area Network (Wireless WAN), where Wireless LAN serves as the hot-spot access area for short-range and very high speed; Wireless MAN serves as the metropolitan-wide access network with high data rate and Wireless WAN provides the national-wide network with relatively low data rate. The substantial technical challenge is to design and implement the security architectures and protocols across such heterogeneous networks taking into account the seamless mobility, scalability and performance efficiency.

4.2 Security-Mobility Management Interaction and Security-Energy Tradeoff

The performance of security management has a close interaction with the framework of mobility management. Mobility management includes two components: location management and handoff management [1]. There are two operations in the location management: updating the UE location and paging the UE. In UMTS, SGSN shall authenticate an UE when the SGSN receives an "Initial L3 message" sent from UE. This message is triggered by the actions, including location update request, connection management request, routing area update request, attach request, paging response. It is clear that all these events are closely relevant to the user's mobility management architecture and mechanism. In [16], Liang and Wang constructed an analytical model to evaluate the impact of authentication on the security and QoS. The authors introduced the system model based on the widely used challenge/response mechanism. Then, a concept of security level is introduced to describe the different level of communication protection with regard to the nature of security, i.e., information secrecy, data integrity, and resource availability. By taking traffic and mobility patterns into account, the technique establishes a quantitative connection between the security and QoS through the authentication and facilitates the evaluation of overall system performance under diverse security levels, mobility and traffic processes.

Normally, an UE is powered by battery and hence the mechanism in efficiently utilizing the limited energy is becoming very important. In case of more frequent authentication to increase the security, the UE will consume more energy. With fewer authentications incurring potential vulnerability, the UE is able to enlarge its lifetime before re-charging. As a consequence, there is a tradeoff between the security and energy management. In [18], Potlapally et al. provided energy consumption empirical measurements for a variety of ciphers, hash functions, and signature algorithms. Based on the observations, the study presented some reasoning about the energy-security tradeoffs in determining key length. However,

no analytical models have been proposed to evaluate the energy-security tradeoffs or make the intelligent decision on tradeoff.

4.3 Higher Security Protocols

Although AKA has been standardized, the protocol has two significant weaknesses: 1) HLR/AuC does not verify whether the information sent from the VLR/SGSN is valid or not. That is, AKA has assumed that the link between VLR/SGSN and HLR/AuC is adequately reliable; 2) for the UMTS integrity protection mechanism, integrity key is transmitted without encryption and the user data are not protected. New strategies shall be designed to address these issues.

In [14], Harn and Hsin identified and discussed the inefficiency and complexity in keeping and managing the sequence number during the network authentication. Based on the combination of hash chaining and keyed-hash message authentication code techniques, an enhanced scheme is proposed to simplify the protocol implementation and simultaneously provide strong periodically mutual authentication.

In [21], Zhang and Fang showed that the 3GPP AKA protocol is vulnerable to a variant of the fake base station attack. The vulnerability allows an adversary to redirect user traffic from one network to another and to re-use corrupted authentication vectors from one network to all other networks. To address such security problems in the current 3GPP AKA, the authors presented a new authentication and key agreement protocol AP-AKA which defeats redirection attack and drastically lowers the impact of network corruption.

4.4 Security Protocols Performance

Security architecture and protocol are normally evaluated to guarantee the security, confidentiality and integrity requirement. Recently, a few studies have appeared to investigate the authentication signaling traffic performance due to the rapidly increasing number of subscribers and consequently potentially high authentication requests and heavy burden on the signaling networks. In [17], Lin and Chen argue the disadvantages in fetching the const number of AV from HLR/AuC. Based on the observations of the mobility pattern, the authors proposed an adaptive scheme to generate an optimal number of AV array, which is able to significantly reduce the authentication signaling traffic and hence save the limited bandwidth utilization. In [20], Zhang and Fujise argue the long delay problem and proposed a mechanism to address the issue. In particular, when the two entities SGSN and HLR/AuC locate far away from each other, the response for available authentication vector may be potentially very long. The consequence of long delay includes call blocking and location update failure, and hence degraded QoS. To address this problem, the study proposed a enhanced scheme to fetch AV earlier before all AVs are used up. Comparing with the original 3GPP Technical Specification TS33.102, the proposed strategy is able to achieve very low probability in waiting for an available AV with negligible increased signaling overhead and low storage cost.

It is proposed that security protocols performance should be evaluated from the security perspective and also from the signaling overhead point of view. New security protocols should consider to combat potential vulnerability as well as to introduce low additional signaling cost.

5 Conclusion

This paper gives an overview on the security management in the next generation wireless networks. The authentication and key agreement (AKA) process is described and its extension in GPRS authentication and IMS authentication are further discussed in detail. The identified research challenges shall serve as the guidance for the further study to propose more efficient security protocols taking into account the network architecture heterogeneity, the energy-security tradeoffs, the mobility-security interaction and comprehensive performance evaluation.

References

[1] 3GPP, *3rd Generation Partnership Project; Technical Specification Core Network; Mobile Application Part (MAP) Specification (Release 1999)*, Technical Specification 3G TS 29.002 V3.7.0 (2000-12), 2000.

[2] 3GPP, *3rd Generation Partnership Project; Technical Specification Group Core Network; Mobile Radio Interface Layer 3 Specification; Core Network Protocols Stage 3 for Release 1999*, 3G TS 24.008 version 3.6.0 (2000-12), 2000.

[3] 3GPP, *3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; 3G Security; Security Architecture*, Technical Specification 3G TS 33.102 V3.7.0 (2000-12), 2000.

[4] 3GPP, *3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; General Packet Radio Service (GPRS); Service Description; Stage 2*, Technical Specification 3G TS 23.060 version 3.6.0 (2001-01), 2000.

[5] 3GPP, *3rd Generation Partnership Project; Technical Specification Core Network; Cx and Dx Interfaces Based on the Diameter Protocol; Protocol Details*, Technical Specification 3G TS 29.229 V5.3.0 (2003-03), 2003.

[6] 3GPP, *3rd Generation Partnership Project; Technical Specification Core Network; IP Multimedia Subsystem Cx and Dx Interfaces; Signaling Flows and Message Contents (Release 5)*, Technical Specification 3G TS 29.228 V5.4.0 (2003-06), 2003.

[7] 3GPP, *3rd Generation Partnership Project; Technical Specification Group Core Network; Signaling Flows For the IP Multimedia Call Control Based on*

SIP and SDP; Stage 3, 3GPP TS 24.228 version 5.5.0 (2003-06), 2003.

[8] 3GPP, *3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; 3G Security; Access Security for IP-based Services*, Technical Specification 3G TS 33.203 V5.5.0 (2003-03), 2003.

[9] 3GPP, *3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; IP Multimedia Subsystem Stage 2*, Technical Specification 3G TS 23.228 version 6.2.0 (2003-06), 2003.

[10] 3G TS 33.105, *3G Security; Cryptographic Algorithm Requirements*.

[11] 3G TS 35.205, *3G Security; Specification of the MILENAGE Algorithm Set: An Example Algorithm Set for the 3GPP Authentication and Key Generation Functions f1, f1*, f2, f3, f4, f5, and f5*; Document 1: General*.

[12] 3G TS 35.206, *3G Security; Specification of the MILENAGE Algorithm Set: An Example Algorithm Set for the 3GPP Authentication and Key Generation Functions f1, f1*, f2, f3, f4, f5, and f5*; Document 2: Algorithm Specification*.

[13] *China Wireless Telecommunication Standard; 3G digital cellular telecommunications system; Security related network functions (Release 3)*, CWTS TSM 03.20 V3.0.0 (2002-08).

[14] L. Harn and W. J. Hsin, "On the security of wireless networks access with enhancements," in *Proceedings of WiSE'03*, pp. 88-95, 2003.

[15] http://www.3gpp.org; http://www.3gpp2.org

[16] W. Liang and W. Wang, "A Quantitative Study of Authentication and QoS in Wireless IP Networks," in *Proceeding of IEEE INFOCOM'05*, pp. 1478-1489, Miami, FL, USA, Mar. 2005.

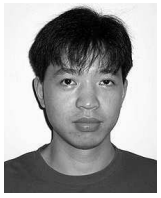
[17] Y. Lin and Y. Chen, "Reducing authentication signaling traffic in third-generation mobile network," *IEEE Transactions on Wireless Communication*, vol. 2, no. 3, pp. 493-501, May 2003.

[18] N. R. Potlapally et al., "Analyzing the energy consumption of security protocols," in *Proceedings of the International Symposium on Low Power Electronics and Design*, ACM Press, pp. 30-35, 2003.

[19] J. Rosenberg et al., *SIP: Session Initiation Protocol*, IETF, RFC 3261, 2002.

[20] Y. Zhang and M. Fujise, "An improvement for authentication protocol in third-generation wireless networks," to appear in IEEE Transactions on Wireless Communication.

[21] M. Zhang and Y. Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," *IEEE Transactions on Wireless Communication*, vol. 4, no. 2, pp. 734-742, Mar. 2005.



Yan Zhang received the B.S. degree in communication engineering from the Nanjing University of Post and Telecommunication; the M.S. degree in electrical engineering from the Beijing University of Aeronautics and Astronautics, China; and a PhD degree in School of Electrical & Electronics Engineering, Nanyang Technological University, Singapore. Since Aug. 2004, he has been working with the Wireless Communications Laboratory, National Institute of Information and Communications Technology. He is on the editorial board of International Journal of Network Security. He is currently serving the lead editor for two books (CRC Press, 2006). His research interests include resource, mobility and security management in wireless mobile networks. He is a member of IEEE and IEEE ComSoc.

Masayuki Fujise received the B.S., M.S. and Dr. Eng. degrees, in communication engineering from Kyushu University, Fukuoka, Japan, in 1973, 1975 and 1987, respectively and the M. Eng. degree in electrical engineering from Cornell University, Ithaca, NY, in 1980. He joined KDD (Kokusai Denshin Denwa Co. Ltd.) in 1975 and was with the R&D Laboratories being engaged in research on optical fiber measurement technologies for optical fiber transmission systems. In 1990, he joined ATR (Advanced Telecommunications Research Institute International) Optical and Radio Communications Research Laboratories Kyoto as a department head, where he managed research on optical inter-satellite communications and active array antenna for mobile satellite communications. He joined CRL (Communications Research Laboratory) Independent Administrative Institution of Japan in 1997. He is now the research supervisor in CRL Yokosuka Radio Communications Research Center and the director of Wireless Communications Laboratory in Singapore. Dr. FUJISE is the recipient of the Jack Spergel Memorial Award of the 33rd International Wire & Cable Symposium in 1984 and he is a member of the IEICE Japan and the IEEE.