Temporary Internet Access for Authentication and Key Agreement for LTE Networks

Xue Jun Li[1], Maode Ma[2], and Jiecheng Xie[2]

[1] Department of EEE, Auckland University of Technology, New Zealand
xuejun.li@aut.ac.nz
[2] School of EEE, Nanyang Technological University, Singapore
emdma@ntu.edu.sg, jcxie@ntu.edu.sg

Abstract. Evolved Packet System-Authentication and Key Agreement (EPS-AKA) is the security protocol in Long-Term Evolution (LTE). However, it is still vulnerable to user identity attacks and fake eNBs. Efficient EPS-AKA (EEPS-AKA) was proposed with some improvements. Nevertheless, the EEPS-AKA is vulnerable to denial-of-service (DoS) attacks and fake eNBs, despite of some minor flaws in its procedures. In this paper, we propose Temporary Internet Access (TIA)-AKA to: (1) prevent user identity disclosure by implementing some additional steps, which allows a user equipment (UE) to request a temporary UE identity to access Internet; and (2) authenticate the Mobility Management Entity (MME) through the validity of the assigned IP address. Physical address and simple password exponential key exchange (SPEKE) method are combined into the proposed TIA-AKA. Efficiency analysis suggests the TIA-AKA provides a fully protection on the user identity and prevent the DoS attack, at the expense of increased bandwidth consumption and processing delay.

Keywords: wireless communications, long term evolution, security attack, DoS attack, authentication and key agreement

1 Introduction

Long Term Evolution (LTE) was proposed to support high data rate, low latency, multimedia traffic for future generation of cellular networks. As shown in Fig. 1, a LTE network consists of the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and the Evolved Packet Core (EPC). E-UTRAN includes evolved nodes B (eNBs), which communicate with user equipments (UEs). The EPC is a fully packet-switched backbone network in LTE. Voice service will be handled by the IP Multimedia Subsystem (IMS) network. The EPC consists of a Mobility Management Entity (MME) and Serving Gateway (SGW), a Packet Data Network (PDN) gateway together with Home Subscriber Server (HSS). When a UE connects to the EPC, the MME performs a mutual authentication with the UE [6]. The SGW forwards user data packets. The PDN GW allows a UE to connect to external packet data networks and allocates IP address to the

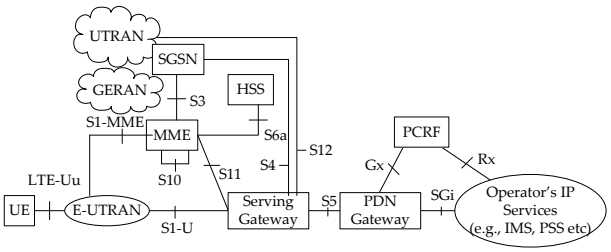

Fig. 1. LTE architecture of E-UTRAN and EPC [13]

UE [12]. With the fast deployment of 4G LTE networks, their vulnerabilities to certain security attacks attracted significant research interests.

In this paper, we study existing security schemes in LTE and propose a new scheme to improve the performance. Section 2 presents the related work, followed by the review of EEPS-AKA in Section 3. Section 4 presents our proposed scheme and Section 5 discusses its formal verification and performance evaluation. Section 6 concludes the paper with possible future work.

2 Related Work

The current security protocol adopted in LTE is Evolved Packet System-Authentication and Key Agreement (EPS-AKA), which evolved from 2G-AKA, 3G-AKA to its current form. However, it is still vulnerable to user identity attacks and fake eNBs. A UE will perform a new registration every time it connects to a new MME due to the fact that the new MME cannot obtain the UE's old Globally Unique Temporary Identifier (GUTI) to retrieve its International Mobile Subscriber Identity (IMSI). The user identity can be revealed when the IMSI is sent in plaintext during the registration process, which allows user identity attack. Similarly, IMSI may be sent to the fake eNB if it acts as a new MME by blocking the signal of real eNBs.

Several solutions were proposed to address these drawbacks. A comprehensive survey of existing researches and studies of LTE and LTE-A networks on security aspects was presented in [6]. In [7], EAP-FAKA was proposed to reduce the authentication delay and signaling cost. However, EAP-FAKA is vulnerable to fake eNBs. In [10], I-AKA with GUTI was proposed to prevent DoS attacks. However, it cannot protect user identity when a UE registers for the first time. In [16], SE-EPS-AKA was proposed based on Wireless Public Key Infrastructure (WPKI), which suggests that UE, MME and HSS shall acquire the digital certificate via Certification Agency (CA) before communication. In [1], a new modified attack "Intelligent brute force" was presented. Nevertheless, it did not explain how an intruder knows the algorithm and the user identity is still vulnerable.

In [11], a HSK-AKA was proposed where digital signature is used to prevent malicious MME. However, the IMSI was encrypted with the new secret key and HSS required to know the IMSI in order to retrieve LTE key and calculate this

secret key. Therefore, a contradiction occurs when a HSS cannot retrieve the IMSI, implying that it cannot read the messages from a UE at all. In [5], a solution was proposed to prevent DoS attacks that UE is required to attach its physical address to the authentication request.

The aforementioned protocols focus on securing the IMSI between UE and MME. Nevertheless, none of them aim to authenticate the authenticity of the MME. Thus, a fake eNB can still request the IMSI from UE as long as same protocol is used. In [2], MEPS-AKA was proposed based on the SPEKE method to provide strong mutual authentication between UE and MME, however, it cost more execution time.

3 Review of EEPS-AKA

3.1 Analysis of EEPS-AKA

Efficient EPS-AKA (EEPS-AKA) was proposed to deal with the issue of user identity disclosure [4]. In EEPS-AKA, Extensible Authentication Protocol (EAP)-SPEKE is based on password shared only between peer and authenticator. It is resistant to both active and passive attacks such as man-in-the-middle (MitM), replay, password sniffing and brute force. It generates a strong session key that can be used in data encryption. The password can be saved in a safe manner. Fig. 2 illustrates the mechanism of SPEKE protocol.

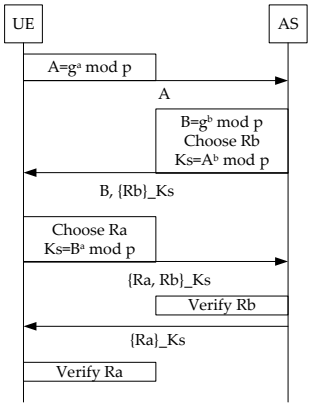

Fig. 2. SPEKE method

In EEPS-AKA, two random values (u and d) are chosen by UE to generate the key A, which makes the shared key always different even though same values (A^u, B^m) are used. The protocol starts when MME computes its value B and sends it to UE with user identity request message. After that, UE computers its value A using two random values (u and d), and the shared secret key K_{um}

using f function, this key is used to protect the IMSI. When MME receives the protected IMSI (PIMSI), it calculates the K_{um} key and forwards it to HSS with other values. HSS and UE can verify each other via the random values computed by K_{um} and K_{uh} keys. To provide perfect forward secrecy, the secret key is used also to compute the generated keys in the later steps such as (IK, CK, and MSK). The details of the EEPS-AKA is in Fig. 3.

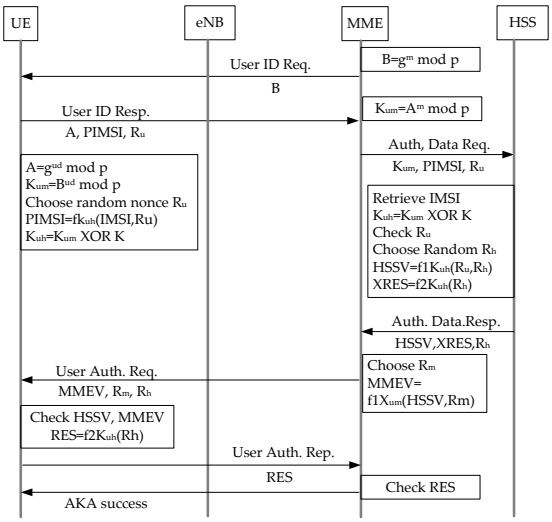

Fig. 3. Overview of EEPS-AKA

3.2 Flaws in the EEPS-AKA

Firstly, two of its computational algorithms the key generation process of EEPS-AKA, $A = g^{ud} \bmod p$ and $K_{um} = B^u \bmod p$, have problems in generating the secret keys. If these expressions are directly used to compute the secret key, it can be derived that:

$$K_{um} = A^m \bmod p = \left(g^{ud} \bmod p\right)^m \bmod p = g^{udm} \bmod p \tag{1}$$

$$K'_{um} = B^u \bmod p = (g^m \bmod p)^u \bmod p = g^{um} \bmod p \tag{2}$$

Obviously, K_{um} is different from K'_{um}. The proposed protocol cannot generate common session keys for UE and MME to communicate with each other, thus the MME cannot decrypt new messages received from UE. The mutual authentication between UE and MME fails at the very beginning. However, further analysis shows that the SPEKE is applicable in generating the session keys.

Assume random values u, d in UE and m in MME, the following algorithms can be used to generate the session keys:

$$K_{um} = A^m \bmod p = \left(g^{ud} \bmod p\right)^m \bmod p = g^{udm} \bmod p \tag{3}$$

$$K_{um}^{'} = B^{ud} \bmod p = (g^m \bmod p)^{ud} \bmod p = g^{udm} \bmod p \tag{4}$$

Even though the idea is proved to be feasible, using two random variables in UE makes no sense in improving the SPEKE method. It may even result in wrong session keys if the g^{ud} or g^{udm} is larger than p as the previous assumption is valid only when g^{ud} or g^{udm} is smaller than p according to MATLAB simulations.

Secondly, the EEPS-AKA can generate strong session keys between UE and MME, which means that the messages between UE and MME cannot be revealed. Nevertheless, EEPS-AKA is still vulnerable to fake eNBs. The EEPS-AKA focuses on the protection of user identity rather than preventing DoS attacks, which can be launched with legitimate UEs. However, the detailed efficiency evaluation and simulation is not performed for EEPS-AKA in [4].

4 Proposed TIA-AKA Scheme

4.1 Motivation of TIA-AKA

Currently, there is no perfect solution to the problem of fake eNBs in LTE. It motivates us to propose Temporary Internet Access Authentication and Key Agreement (TIA-AKA) protocol, which utilizes the IP allocation scheme in LTE to distinguish fake eNBs.

4.2 Proposed TIA-AKA

TIA-AKA is based on EPS-AKA protocol and the SPEKE method used in EEPS-AKA. In addition, a special server is proposed to enhance the verification mechanism. TIA-AKA features a new mechanism for the UE to identify fake eNBs. UE requests temporary user identity for Internet access to check the authenticity of the MME/eNBs. It also combines the SPEKE method with MAC address to protect IMSI and prevent DoS attacks. As shown in Fig. 4, there are two sections and totally 10 steps for the TIA-AKA protocol. The first section is to validate the MME and the second section is mutual authentication among UE, MME and HSS. The 10 steps are:

(1) UE generates random variable u, computes $A = g^u \bmod p$, and sends the authentication request with A and its MAC address to MME via eNB.

(2) When MME receives the authentication request, MME records the MAC address and compares with its memory to avoid DoS attack. If the MAC address is fresh, the MME generates random variable m, computes $B = g^m \bmod p$ and uses the received A to compute the symmetric shared key $K_{um} = A^m \bmod p$. Then, MME sends a temporary identity request to the HHS.

(3) Upon receiving the temporary identity request, HSS generates a temporary identity request, authorizes the identity to be available for around 10 seconds and sends it back to the MME.

(4) The MME encrypts the temporary UE identity with K_{um} and send the message B, $\{TUI\}_{K_{um}}$ to UE.

(5) When UE receives the message B and $\{TUI\}_{K_{um}}$, UE computes symmetric shared key $K_{um} = B^u \bmod p$. UE uses the computed key K_{um} to decrypt the TUI and apply the TUI to request connection on P-GW. If the UE can get a valid IP address and connect to the Internet, the UE confirms that the MME is legitimate MME. *Furthermore, a server of service provider is specially set up for temporary identity authentication.* A special message and expected response with a special symmetric key is stored in SIM card when produced. Once UE accesses the Internet for authentication, it sends the special message with its temporary identity to the server. If the response tells that the identity is legitimate, UE confirms that MME is legitimate. Then, UE sends its IMSI, registration request and MAC address encrypted with the K_{um} to the MME.

(6) MME compares the MAC address again to prevent DoS attack and forwards the IMSI, SNID and n to HSS if the request is fresh.

(7) Upon receiving the authentication request from the MME, the HSS first verifies the IMSI and SNID and uses the retrieved LTE key and generated random RAND and SQN to create XRES, AUTN, CK and IK. Then, a top-level key (K_{ASME}) is calculated through Key Derivation Function (KDF) with the SNID, CK and IK. The HSS forms n AVs and sends them back to the MME. The $AV_i = (\mathrm{RAND}_i, \mathrm{AUTH}_i, \mathrm{XRES}_i, K_{ASME_i}), i = 0, 1, \cdots, n$. MAC = $f_{1k}\,(\mathrm{SQN}||\mathrm{RAND}||\mathrm{AMF})$, XRES = $f_{2k}\,(\mathrm{RAND})$, CK = $f_{3k}\,(\mathrm{RAND})$,IK = $f_{3k}\,(\mathrm{RAND})$,AK = $f_{3k}\,(\mathrm{RAND})$ K_{ASME} = $\mathrm{KDF}\,(\mathrm{SQN} \oplus \mathrm{AK}, \mathrm{SN}, \mathrm{id}, \mathrm{CK}, \mathrm{IK})$, AUTN = SQN $\oplus$ AK||AMF||MAC.

(8) The MME stores the AVs received from the HSS, and selects one of them to use in LTE authentication of the UE. The MME allocates KSI_{ASME}, an index of K_{ASME}, and delivers it instead of K_{ASME} to the UE so that the UE and the MME can use it as a substitute for K_{ASME}. The MME sends KSI_{ASME_i} together with $RAND_i$ and $AUTH_i$ in the Authentication Request to the UE.

(9) Upon receiving the Authentication Request from the MME, the UE extracts the messages from the AUTH to check the received messages with following operations: XAK = f_{5k}(RAND), SQN = XAK $\oplus$ SQN $\oplus$ AK, XMAC = $f_{1k}\,(\mathrm{SQN}||\mathrm{RAND}||\mathrm{AMF})$ =?MAC, XSQN =?SQN. If one of the two checks fail, it delivers Authentication Failure (CAUSE) message; otherwise, it calculates RES=f2k (RAND) and sends Authentication Response with RES back to MME.

(10) Once the MME receives the RES from the UE, it compares the RES with the XRESi of the AV received from the HSS. If RES matches the XRESi, the MME send a success message to UE and the authentication process is completed.

After completion of authentication, the UE derives K_{ASME} with CK, IK, SQN and SN ID. KSI_{ASME} received from the MME is used to represent the index of K_{ASME} and KSI_{ASME} is used during the NAS security setup between the UE and the MME. Note that these procedures are only processed when

the UE registers to the MME and HSS for the first time; after success of the registration, GUTI is used instead of IMSI for other authentication process.

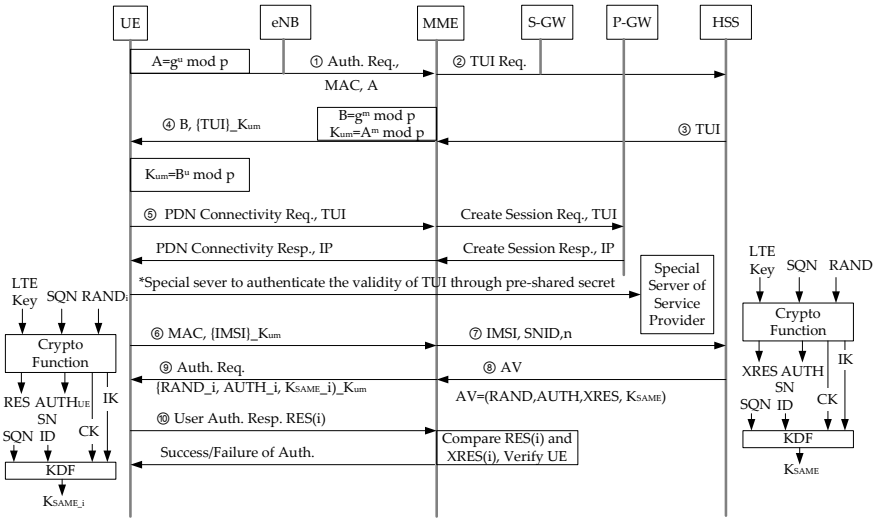

Fig. 4. Overview of proposed TIA-AKA

5 Security Analysis and Performance Evaluation

5.1 Formal Verification of TIA-AKA

The automated validation of Internet security protocols and applications (AVISPA) tool is used for validating the protocols. The AVISPA verification outputs of EEPS-AKA and TIA-AKA are shown in Fig. 5(a) and Fig. 5(b), respectively. From the execution outputs, we can see that the TIA-AKA is safe and it achieves the specified goals.

5.2 Performance Evaluation of TIA-AKA

Table 1 summarizes the length of authentication parameters [14]. For EPS-AKA, the bandwidth requirement [18] is given by

$$BW_{EPS-AKA} = (963 + 608n)\, N_{avg,AEPH} \tag{5}$$

where $N_{avg,AEPH}$ is the average number of authentication event per HSS. Similarly, for the proposed TIA-AKA, the bandwidth requirement is given by

$$BW_{TIA-AKA} = (1510 + 608n)\, N_{avg,AEPH} + (393)\, N_{avg,AEPM} \tag{6}$$

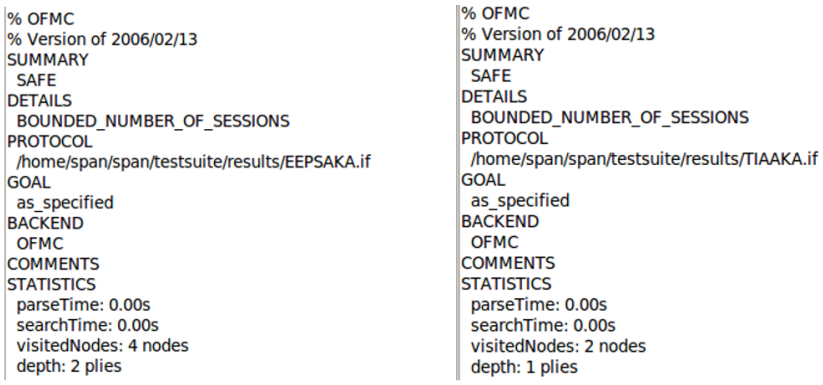

Fig. 5. AVISPA outputs of (a) EEPS-AKA and (b) TIA-AKA

where $N_{avg,AEPM}$ is the average number of authentication event per MME. In equation (6), the last term corresponds to additional bandwidth consumption for UE to authenticate the MME through the Internet under TIA-AKA. For simplicity, as long as the UE can receive an IP address and establish the default bearer, it considers that the MME is legitimate.

Table 1. Length of Authentication Parameters

Parameters	Length (bits)	Parameters	Length (bits)
RES, MAC, Type, TAl, IMSI	64	AMF	16
K (LTE K), RAND, CK, IK	128	SQN,AK	48
KSI_{ASME}	3	K_{ASME}	256
service request	8	AUTN	128
physical address	48	AV	608

The simulated network consists of one MME area, dividing into three tracking area (TA). Each TA contains seven eNBs. For TIA-AKA, the authentication processes is done only in its first registration. The following parameters are used: (1) average velocity V for UE; (2) movement direction of UE is uniformly distributed over [0, 2π]; (3) UEs are uniformly populated with the density within the area, ρ; (4) The radii of eNB area, TA and MME are L_1, L_2 and L_3, respectively. The average number of active mobile crossing the area boundary of length L, is given by $R = \rho VL/\pi$. Note that handover happens when UE is in active mode; Tracking Area Update (TAU) happens when UE is in idle mode; registration happens when MS is switched on or moved from one SN to another.

The simulation covers two scenarios, urban area and suburban area. For urban area, $\rho = 1000$ people/km^2, $V = 40$ km/h, $L_1 = 800$m. Number of MME is 30. From Fig. 4, we know that $L_3 \approx 4.5 * L_1$. Therefore, the average number of authentication request in the HSS is about 382/second. The total bandwidth consumptions for EPS-AKA and TIA-AIA are 382*(963+608n) bps and 382*(1510+393+608n) bps, respectively. For suburban area, $\rho = 100$ people/km^2, $V = 80$ km/h, L_1= 1500m. The number of MME is 5. Therefore the average number of authentication request in the HSS is about 24/second. The total bandwidth consumptions for EPS-AKA and TIA-AIA are 24*(963+608*n) bps and 24*(1510+393+608*n) bps, respectively.

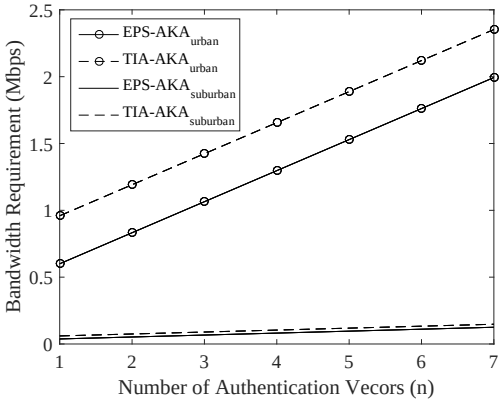

Fig. 6. The bandwidth consumption simulation results of TIA-AKA

From Fig. 6, it can be seen that when more authentication requests occur, the bandwidth consumption of TIA-AKA raises sharply as n grows. Due to the extra message size through MME, the difference between bandwidth consumption of EPS-AKA and that of TIA-AKA increases with the increase of authentication requests. Table 2 compares message sizes of different protocols with n=1.

Table 2. Performance Comparison with n=1

Protocol	EPS-AKA	EEPS-AKA	SE-AKA	G-AKA	TIA-AKA
Message Bits	1571	1776	2184	1888	2511
Excess Percentage	-	13%	39%	20%	60%

6 Conclusion

TIA-AKA is proposed to prevent user identity disclosure and fake eNBs. Efficiency analysis shows that TIA-AKA provides a fully protection on the user identity and prevents the DoS attack through the MAC address checkout, at the expense of increased bandwidth consumption and authentication delay. Our future work will be improvement on the efficiency of TIA-AKA with group authentications.

References

1. J. B. B. Abdo, H. Chaouchi, and M. Aoude. Ensured confidentiality authentication and key agreement protocol for EPS. In *RELABIRA'12*, 2012.
2. M. A. Abdrabou, A. D. E. Elbayoumy, E. Abd El-Wanis. LTE authentication protocol (EPS-AKA) weaknesses solution. In *ICICIS'15*, pp. 434–441, 2015.
3. T. Ahmed, D. Barankanira, S. Antonie, Xiaofeng Huang, and Herve Duvocelle. Inter-system mobility in evolved packet system (EPS): Connecting non-3GPP accesses. In *ICIN'10*, 2010.
4. K. A. Alezabi, F. Hashim, S. J. Hashim, and B. M. Ali. An efficient authentication and key agreement protocol for 4G (LTE) networks. In *IEEE Region 10 Symposium'14*, pp. 502–507, 2014.
5. C.-G. Apostol and C. Racuciu. Improving LTE EPS-AKA using the security request vector. In *ECAI'15*, 2015.
6. J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo. A survey on security aspects for LTE and LTE-A networks. *IEEE Comms. Surveys & Tutorials*, 16(1):283–302, 2014.
7. Y. EI Hajjaji EI Idrissi, N. Zahid, and M. Jedra. Security analysis of 3gpp (LTE) – WLAN interworking and a new local authentication method on EAP-AKA. In *FGCT'12*, pp. 137–142, 2012.
8. D. Forsberg, L. Huang, K. Tsuyoshi, and S. Alanaram. Enhancing security and privacy in 3GPP E-UTRAN radio interface. In *PIMRC'07*, 2007.
9. J. D. Gibson. *Mobile Communication Handbook*. CRC Press, USA, 3^{rd} ed., 2013.
10. L. Gu and M. A Gregory. A green and secure authetication for the 4^{th} generation mobile network. In *ATNAC'11*, pp. 1–7, 2011.
11. K. Hamandi, I. Sarji, A. Chehab, I. H. Elhajj, and A. Kayssi. Privacy enhanced and computationally efficient hsk-aka lte scheme. In L. Barolli, F. Xhafa, M. Takizawa, T. Enokido, and H. H. Hsu, editors, *WAINA'13*, pp. 929–934. IEEE, 2013.
12. ETSI. Digital cellular telecommunication system (phase 2+)(GSM); universal mobile telecommunications system (UMTS); LTE; network architecture, May 2017.
13. ETSI. Lte; general packet radio service (GPRS) enhancements for evolved universal terrestrial radio access network (E-UTRAN) access, Oct. 2017.
14. ETSI. Universal mobil telecommunications system (UMTS); lte; 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, Apr. 2017.
15. G. M. Køien. Mutual entity authentication for LTE. In *IWCMC'11*, 2011.
16. X. H. Li and Y. J. Wang. Security enhanced authentication and key agreement protocol for LTE/SAE network. In *WiCOM'11*, 2011.
17. H. Mun, K. Han, and K. Kim. 3G-WLAN interworking: security analysis and new authentication and key agreement based on EAP-AKA. In *WTS'09*, 2009.

18. M. Purkhiabani and A. Salahi. Enhanced authentication and key agreement procedure of next generation evolved mobile networks. In *ICCSN'11*, pp. 557–563, 2011.
19. D. Yu and W. Wen. Non-access-stratum request attack in E-UTRAN. In *ComComAp'12*, pp. 48–53, 2012.