Applied Mathematical Sciences, Vol. 9, 2015, no. 47, 2337 - 2349
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ams.2015.53215

A Robust Secure DS-AKA with Mutual Authentication for LTE-A

M. Prasad and R. Manoharan

Department of Computer Science and Engineering
Pondicherry Engineering College
Puducherry 605 014, India

Abstract

The authentication and key agreement (AKA) protocol for Long Term Evolution-Advanced (LTE-A) which is proposed to solve the vulnerabilities found in previous communication systems such as 2G and 3G systems. They still contain the vulnerabilities like redirection and man-in-the-middle attack. They gave way to the eavesdroppers to utilize and misuse the subscribers resources and make the communication system to mischarge the customers. In this paper we propose an authentication key agreement algorithm which is secure and able to solve the vulnerabilities in the communication system. This reduces the bandwidth utilization for authentication and number of transactions required for authentication is reduced.

Keywords: LTE-A, eNB, AKA, ElGamal, Diffie-Hellman Key Exchange

1 Introduction

Security is a critical issue in mobile radio applications, for users and providers of communication system. The LTE-A architecture consist of two main components the eNB and the Evolved Packet Core. The eNB consist of the radio access network, the antenna and the air medium for transportation [1] [13]. The User Equipment (UE) connected to the antenna which is responsible for the UE is authenticated to the core network. An evolved Node B - eNB - is the

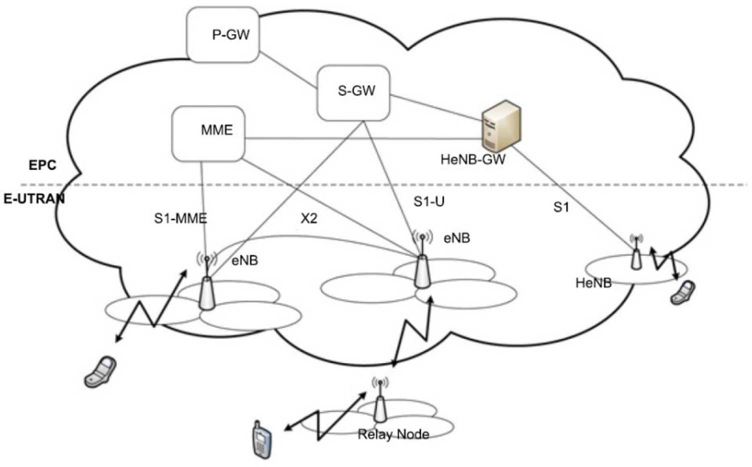


Figure 1: LTE-A Architecture

part of the LTE-A system which access the radio. Each eNB contains radio transmitter, receiver, control section and power supply.

In addition eNBs contain resource management and logic control functions that have been separated into base station controllers (BSCs) or radio network controllers (RNCs). eNB functions include radio resource management - RRM, radio bearer control, radio admission control - access control, connection mobility management, resource scheduling between UEs and eNB radios, header compression, link encryption of the user data stream, packet routing of user data towards its destination, scheduling and transmitting paging messages (incoming calls and connection requests), broadcast information coordination(system information), and measurement reporting (to assist in handover decisions). Figure 1 shows the LTE-A architecture.

2 RESEARCH BACKGROUND

In LTE-A, both the air interface and the radio access network are being upgraded or refined, but so far the core network architecture, i.e. the EPC is not undergone major changes [11]. Mobile management entity (MME) [8] which is a processing element that can be used to find, route, and maintain and transfer communication connections to UE. The MME can perform end to end connection signaling and security services between core networks. Mode access control to the UE is performed when it is not connected [7] [14] [10] [19].

The MME maintains location information about devices and determine which gateway will be used to connect mobile devices to other networks. MME is the core network equipment is responsible for UE management. When the UE is moving around the radio network and choosing which is going to connect the data traffic for the particular UE. When the UE is connected with an eNB via the radio interface, the antenna first forwards all the traffic to the MME. The main role of MME is to facilitate the verification of the UE authentication and authorization credentials, based on UE identity and credentials stored in Home Subscriber Server (HSS). MME is the control plane dedicated entity it didnt involve in the user plane traffic flow.

2.1 GSM security features:

International Mobile Subscriber Identity (IMSI) function is to avoid an interceptor of the mobile traffic being able to identify which subscriber is using a given resource on the radio path [15]. It never transmits in clear text in any signaling message. Instead of IMSI Temporary Mobile Subscriber Identity (TMSI) is used to identify a mobile subscriber on the radio path. The Visitors Location Register (VLR) allots the TMSI where MS is registered. New TMSI is allotted on every location update by VLR [22].

The key Ki is allotted with the IMSI, at the subscription time. Ki is stored in subscriber SIM and in an AuC belonging to the MSs HPLMN. A PLMN may contain one or more AuCs [22].

The information which follows is considered sensitive and must be protected against eavesdropping:

- Signaling information elements.
- For confidentiality TMSI must be transferred in protected mode at allocation time.
- User data.

The MS is authenticated to the BS, but in this the BS is not authenticated to the MS. Here mutual authentication is not provided so there is possibility of attacks where a malicious third party masquerades as a BS to one or more MSs. The general LTE-AKA is shown in figure 2.

LTE-AKA [17]is vulnerable to false base station attack [20]; it allows an adversary to redirect user traffic to other network. In this issue the need of synchronization between mobile station and its home network have to overcome the difficulty for the normal operation of the protocol.

The user has to ensure that authentication information cannot be reused by a serving network. The serving network authenticates the user by verifying the user authentication response, RES, to determine if the user has knowledge of the authentication key.

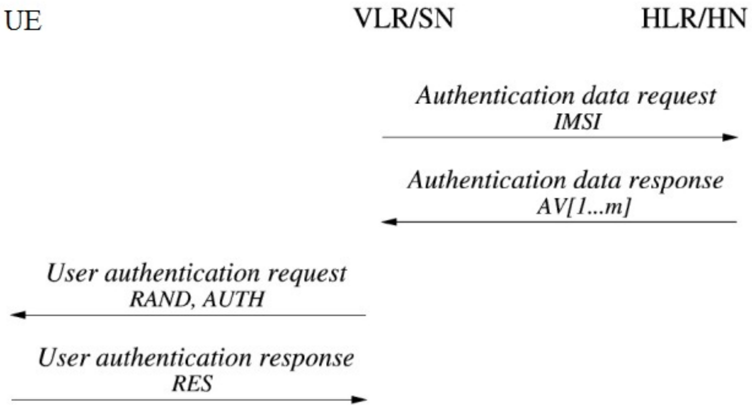

UE
VLR/SN
HLR/HN
Authentication data request
IMSI
Authentication data response
AV[1...m]
User authentication request
RAND, AUTH
User authentication response
RES

Figure 2: LTE-AKA

2.2 Re-direction Attack:

A user is in his home network and needs to establish a communication session with the home network. A device having the functionality of a base station, such a device is called false base station. The device intercepts the connection attempt from the user and makes the user to rely on the radio channel of the base station. Then the authentication is successful in both the sides and subsequent communication will be protected by the established key, likewise the device can re-direct user traffic to the unintended network.

Public-key algorithms are often too inefficient for signing long documents. Digital signature protocols use a cryptographic digest to save time; it is a one-way hash of the document. Instead of the document the hash is signed for verification. The hashing and digital signature algorithms are agreed in advance. The process summary is given below:

1. A one-way hash of the document is produced.
2. The hash is encrypted with the private key, this makes the document signed.
3. The document and the signed hash are transmitted.
4. The recipient produces a one-way hash of the document.
5. Using the digital signature algorithm, the recipient decrypts the signed hash with the sender's public key.

2.3 Digital Signature Standard:

The DSA digital signature is a pair of large numbers represented in a computer as strings of binary digits. The digital signature is computed using a set of rules (i.e., the DSA) and a set of parameters such that the identity of the signatory and integrity of the data can be verified in the digital signature system. The DSA provides the capability to generate and verify signatures. Signature generation makes use of a private key [16] by which digital signature is generated. Signature Verification makes use of a public key but is not the same as, the private key. Every user possesses a private and public key pair of its own. Public keys are assumed signatures for stored as well as transmitted data. All have the rights to verify the signature of a user by employing that user's public key and the signature generation can be performed only by the owners of the user's private key [5].

The integrity of the signed data and the identity of the signatory are authenticated by the DSA. The data was actually signed by the generator of the signature is proved to a third party by the DSA. The DSA is intended for use in electronic mail, electronic funds transfer, software distribution, data storage, electronic data exchange, and other applications which require data integrity assurance and data origin authentication [2].

The DSA may be implemented in software, firmware, hardware, or any combinations. NIST is developing a validation program to test implementations for conformance to this standard.

2.4 Public Key Infrastructure:

Public Key Infrastructure (PKI) [4] is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. The infrastructure of PKI is expected to offer its users the following benefits:

- The quality of information to be sent and received electronically must be sureness.

- The source and destination of that information must be correct and trustable.

- The time and timing of that information sent must be accurate (providing the source of time is known).

- The privacy to that information must be maintained.

- Assurance that the information may be introduced as evidence in a court or law.

PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The user identity must be unique within the network for each CA domain and the binding is established through the registration and issuance process. It depending on the level of assurance that the binding has, which may be carried out by software at a CA, or under human manual supervision. The PKI role gives the assurance to this binding is called the Registration Authority (RA). The RA ensures that the public key is bound to the individual to which it is assigned in a way that ensures non-repudiation [17].

2.5 Certification Authority:

A certificate authority (CA) is an entity that issues digital certificates. The digital certificate checks the ownership of a public key by the named subject of the certificate. This rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. A CA is a trusted third party that is trusted by both the owner of the certificate and the party relying upon the certificate. CAs is characteristic of many public key infrastructure (PKI) schemes [3].

2.6 Verifier:

The verifier is the person or application which checks the contents of the digital certificate and validates the certificate.

3 DL BASED PROTOCOL

In this proposal the Digital Certificate is never be revealed as plain text for the verification and it satisfy the several security requirements:

1. **Man-in-the-middle attack:** It's not possible due to the signature is not passed as plain text and no feasibility of the computation of the private key with their corresponding public key [12].

2. **Unforgeability:** Valid response only generated by the User Equipment.

3. **Nontransferability:** It's not transferable due to personal identification via digital certificate.

Our proposed protocol is built with the combination of the ElGamal digital signature (DL- based) and the Diffie-Hellman Assumption (DHA) [21] [18] [9] [6].

3.1 ElGamal Digital Signature

The ElGamal Signature is a digital signature scheme which is based on the difficulty of the computing discrete logarithm. A variant developed at NSA and known as the Digital Signature Algorithm is much more widely used. There are several other variants. The ElGamal signature scheme allows that a verifier can confirm the authenticity of a message m sent by the signer sent to him over an insecure channel.

Some system parameters like collision-resistant hash function (H), discrete logarithms modulo p (largest prime number), and g <p randomly chosen generator of the multiplicative groups of integers modulo p.

3.1.1 Key generation:

Choose randomly a secret key x
with 1 < x < p − 1.

1. Compute y = gx mod p.
2. The public key is (p, g, y).
3. The secret key is x.

Performed once by signer.

3.1.2 Signature Generation:

Choose a random k
such that 0 < k < p –1 and gcd(k, p –1) = 1.

1. Compute r ≡ gk (mod p).
2. Compute S ≡ (H(m) –xr)k –1 (mod p–1)
3. If S = 0 start over again.

3.1.3 Verification:

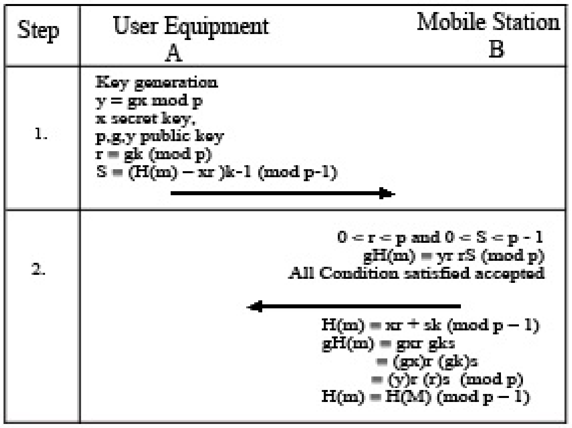
A signature (r,s) of a message m is verified as follows.

1. 0 < r < p and 0 < s < p –1
2. gH(m) ≡ yr rs (mod p)

The verifier accepts a signature if all conditions are satisfied and rejects it otherwise. The signature generation implies

$H(m) \equiv xr + sk$ (mod p-1)
$gH(m) \equiv gxr\ gks$
$\equiv (gx)r\ (gk)s$
$\equiv (y)r\ (r)s$ (mod p)
$H(m) \equiv H(M)$ (mod p-1)

Figure 3 shows the proposed DS-AKA algorithm.



Step	User Equipment A	Mobile Station B
1.	Key generation y = gx mod p x secret key, p,g,y public key r = gk (mod p) S = (H(m) – xr)k-1 (mod p-1) →	
2.	←	0 < r < p and 0 < S < p - 1 gH(m) = yr rS (mod p) All Condition satisfied accepted H(m) = xr + sk (mod p – 1) gH(m) = gxr gks = (gx)r (gk)s = (y)r (r)s (mod p) H(m) = H(M) (mod p – 1)

Figure 3: DS-AKA

3.1.4 DiffieHellman assumption:

Let A and B have their own private keys x_a and x_b and their corresponding public keys,
$y_a = g^{xa}$ modp and $y_b = g^{xb}$ modp

Where p is the largest prime number [5] and g is the multiplicative group modulo p. Only A and B can compute the shared secret $K_{a,b} = y_{b^{xa}} = y_{a^{xb}} = K_{b,a}$ mod p. Unable to solve the private key of A and B with the corresponding public key of A and B.

3.1.5 Authentication and Key Agreement Protocol with Digital Signature:

Registration at CA:

Let A be the UE (User Equipment) and B be the MS (Mobile Station) verifier. A needs to register with CA and obtain the digital certificate. The CA generates the digital signature with the Elgamal signature (rA, sA) for the User

Equipment A mA according to equation (1). Since the signature component rA is a random integer and does not depend on mA, it does not need to be kept secret. The signature component sA is a function of the statement. Each owner needs to keep it secret from the verifier in the authentication process.

Protocol:

The authentication and key agreement protocol has the following steps:

1. The user A generates the private key (x) and public key (y) and passes the parameters (rA, sA) to the verifier UE.
2. The computation for signature generation is
   s ≡ (H(m)xr)k-1(mod p-1).
3. The Verifier MS checks the parameters with the computation
   gH(m) ≡ yr rs(mod p).

4 RESULTS AND ANALYSIS

The enhancement of DS-AKA includes the following factors:

4.1 Resistance to redirection attack:

In UMTS AKA, LAI, which identifies the location of the BSS, is not protected and can be altered by hackers with some redirection attack. DS-AKA uses message authentication code, which protect the message integrity of LAI, which preventing the network from redirection attacks.

4.2 Resistance to man-in-the-middle attack:

A man-in-the-middle attack can be established while connecting to a GSM BSS. The payload between the MS and SGSN is negotiated to encrypt. This prevents the communication from being eavesdropped or modified.

4.3 Reduced Bandwidth Consumption:

Using Digital Signature, the proposed protocol allows the HLR/AuC to authorize the SGSN for subsequent and mutual authentication. It reduces the traffic between HLS/AuC and the SGSN and the bandwidth consumption is greatly reduced.

The proposed DS-AKA is simulated in NS3.14. The main parameter taken in this simulation is time and overhead. With respect to time and number

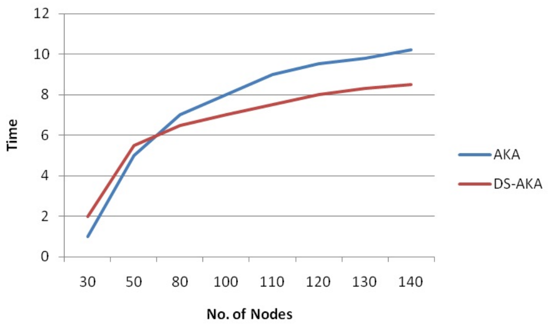


Figure 4: Comparison of AKA's

of nodes are taken into consideration initially DS-AKA requires more time to authenticate than 3GPP AKA. By increasing the number of nodes in an eNB the DS-AKA gone steady when compared to 3GPP AKA. The graph obtained is shown in Figure 4.

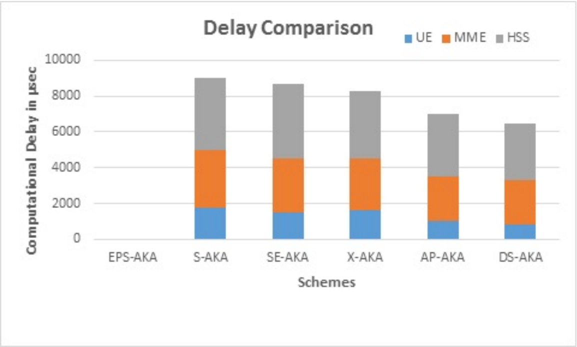


Figure 5: Computational delay

The computational delay in various available AKA schemes and DS-AKA scheme is shown in figure 5. The number of messages transferred for authentication between the eNB and UE is reduced and encrypted. The original key never sent upon the channel between the eNB and UE. The original key is computed in UE and send to eNB. Another key is generated and computed by the eNB and send to UE. The key exchange is based upon the Diffie Hellman Key Exchange algorithm. The original key is never exposed in the radio signals. It makes the proposed protocol more secure.

5 CONCLUSION

Security and implementation requirements for personal communication systems have been discussed. To provide better protection, DS-AKA protocols with more security features, which reduce the bandwidth utilization and resistant to redirection and man-in-the-middle attack and protect sensitive data without involving complicated computations, were proposed and then analyzed. Here we summarize the properties of the proposed protocols:

A compromised session key does not compromise the contents of the following sessions, nor does it lead to the masquerading of either the subscriber or the service provider.

Computation on the subscriber is simple, so that battery of the mobile unit can last longer.

Number of interactions among the UE and the MS are minimized. It speeds up the verification and therefore reduces the total delay of validation.

References

[1] *3g the future of communications.*

[2] Sathish Babu B. and Pallapa Venkataram, *A dynamic authentication scheme for mobile transactions*, International Journal of Network Security **8** (2009), no. 1, 59–74.

[3] Kou-Min Cheng, Ting Yi Chang, and Jung-Wen Lo, *Cryptanalysis of security enhancement for a modified authenticated key agreement protocol*, IJ Network Security **11** (2010), no. 1, 55–57.

[4] S Farrell S Boeyen R Housley D. Cooper S. Santesson and W Polk, *Internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile*, Tech. report, May 2008.

[5] W Diffie and M E Hellman, *New directions in cryptography*, Information Theory, IEEE Transactions on **22** (1976), no. 6, 644–654.

[6] Taher Elgamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Transactions on Information Theory **31** (1985), 469–472.

[7] K. Hamandi, I Sarji, IH. Elhajj, A Chehab, and A Kayssi, *W-aka: Privacy-enhanced lte-aka using secured channel over wi-fi*, Wireless Telecommunications Symposium (WTS), 2013, April 2013, pp. 1–6.

[8] Yu-Lun Huang, C Y Shen, Shiuhpyng Shieh, Hung-Jui Wang, and Cheng-Chun Lin, *Provable secure aka scheme with reliable key delegation in umts*, Secure Software Integration and Reliability Improvement, 2009. SSIRI 2009. Third IEEE International Conference on, July 2009, pp. 243–252.

[9] Jayaprakash Kar and Banshidhar Majhi, *A novel deniable authentication protocol based on diffie-hellman algorithm using pairing technique*, Proceedings of the 2011 International Conference on Communication, Computing & Security, 2011, pp. 493–498.

[10] Chengzhe Lai, Hui Li, Rongxing Lu, and Xuemin (Sherman) Shen, *Se-aka: A secure and efficient group authentication and key agreement protocol for* {*LTE*} *networks*, Computer Networks **57** (2013), no. 17, 3492 – 3510.

[11] V.H. MacDonald, *Advanced mobile phone service: The cellular concept*, Bell System Technical Journal **58** (1979), 15–41.

[12] Ulrike Meyer and Susanne Wetzel, *A man-in-the-middle attack on umts*, Proceedings of the 3rd ACM Workshop on Wireless Security (New York, NY, USA), WiSe '04, ACM, 2004, pp. 90–97.

[13] Hyeran Mun, Kyusuk Han, and Kwangjo Kim, *3g-wlan interworking: Security analysis and new authentication and key agreement based on eap-aka*, 2009 Wireless Telecommunications Symposium, WTS 2009, 2009.

[14] Hsia Hung Ou, Iuon Chang Lin, Min Shiang Hwang, and Jinn K. Jan, *Tk-aka: Using temporary key on authentication and key agreement protocol on umts*, International Journal of Network Management **19** (2009), 291–303.

[15] Martin Sauter, *From gsm to lte*, Wiley, 2011.

[16] K S Selvi and T Vaishnavi, *Rabin publickey cryptosystem for mobile authentication*, Advances in Engineering, Science and Management (ICAESM), 2012 International Conference on, 2012, pp. 854–860.

[17] Dong Hwi Seo and P Sweeney, *Simple authenticated key agreement algorithm*, Electronics Letters **35** (1999), no. 13, 1073–1074.

[18] A Upadhyay, J.K. Sahoo, and V. Bajpai, *A novel architecture for secure communications in mobile systems*, Internet Technology And Secured Transactions, 2012 International Conference for, Dec 2012, pp. 801–805.

[19] Shuhua Wu, Yuefei Zhu, and Qiong Pu, *Security analysis of a cocktail protocol with the authentication and key agreement on the umts*, IEEE Communications Letters **14** (2010), 366–368.

[20] Zhao Yao, Lin Chuang, and Yin Hao, *Security authentication of 3g-wlan interworking*, Proceedings - International Conference on Advanced Information Networking and Applications, AINA, vol. 2, 2006, pp. 429–433.

[21] Dongfang Zhang, Ru Zhang, Xinxin Niu, Yixian Yang, and Zhentao Zhang, *A new authentication and key agreement protocol of 3g based on diffie-hellman algorithm*, ICCET 2010 - 2010 International Conference on Computer Engineering and Technology, Proceedings, vol. 2, 2010.

[22] Xiankun Zheng and Changjiang Liu, *An improved authentication and key agreement protocol of 3g*, Education Technology and Computer Science, 2009. ETCS '09. First International Workshop on, vol. 2, 2009, pp. 733–737.

Received: December 15, 2014; Published: March 21, 2015