Analysis of UMTS (3G) Authentication and Key Agreement Protocol (AKA) for LTE (4G) Network

Anilmit Choudhary
Computer Science Department
Shoolini University
Solan, (H.P), India
anilmitchoudhary@gmail.com

Randhir Bhandari
Computer Science Department
Shoolini University
Solan, (H.P), India
randhir.492@shooliniuniversity.com

Abstract: Technological and security enhancements in third generation (3G) architecture led to the development of the fourth generation (4G) technology. 4G is developed and standardized by the 3GPP which is a fully IP based topology and also referred to as the future communication technology. 3GPP provided LTE (Long Term Evolution) usually referred to as the standard for fourth generation telecommunications. This paper reviews the core architecture of the 4G network and also reviews the Authentication and key agreement (AKA) protocol as the access mechanism to a 4G network which shows the strong security aspects of the fourth generation technology.

Keywords: *3G, UMTS AKA, 4G (LTE), 4G Security Mechanism, 4G Architecture.*

*****

I. INTRODUCTION

Technology advancements in field of mobile technology have gone through some major enhancements due to the security flaws in each predecessor generation. Security flaws in the second generation (GSM) led to the development of third generation (UMTS). Similarly, flaws in the security architecture of 3G led to the development of the next generation technologies referred to as fourth generation technology (4G). GSM was the standard to the second generation mobile technologies. Digital signals were used to transmit information in second generation. 2G technology helped in providing a speed of 40 Kbit/s. It also focused in providing the security regarding the authentication of user equipment but lacked in the authentication of base station which promoted false base station attack. In order to remove the prevalent weakness in the GSM, a more secure advancement was made which resulted in the evolution of third generation technology usually referred to as UMTS, standardized by 3GPP. 3G offers mutual authentication which authenticates both the user as well as the network and removes the so called false base station attack in GSM. It also provide mobile users with the data transmission speed of about 2Mbit/s. Increased data transmission speed with respect to the second generation technology is the major attraction of UMTS[4]. However, a more reliable and requirement of much high speed network technology led to the evolution of next generation technology usually referred to as the fourth generation 4G. A 3GPP standard for fourth generation (4G) is LTE (Long Term Evolution). Other standard for 4G technology include 802.16m usually known as WiMAX standardized by IEEE.

Firstly, we provide a brief introduction about the systematic authentication process of the Authentication and key agreement (AKA) protocol in the third generation (3G) i.e. UMTS framework. A short description of the authentication process involving various steps during mutual authentication in UMTS AKA is provided in this section of paper.

Secondly, we provide the basic core design of a 4G network. In this section core design of the 4G network is being covered in detail along with the user mobile device in a non-roaming scenario [2]. In the next part of this paper we try to review about the 4G security architecture with respect to the well know Authentication and Key Agreement (AKA) protocol. The LTE AKA (AKA for 3GPP 4G network) provides some extra features when compared to the UMTS AKA which helps in providing more security to the user with respect to their authentication to the network.

II. OVERVIEW OF THE UMTS AKA

3G network uses Authentication and Key agreement (AKA) protocol for its mutual authentication process. In mutual authentication process the client authenticates the network by calculating the response (RES) using its secret key and the network authenticates back the client through authentication vectors by comparing response with the expected response(XRES). The mutual authentication process helps in removing the false base station attack which is most prevalent in the GSM framework. Using symmetric cryptography, UMTS AKA shares a secret key with the Mobile station (MS) and the Home Environment (HE) in order to maintain the private information to increase the security aspects.

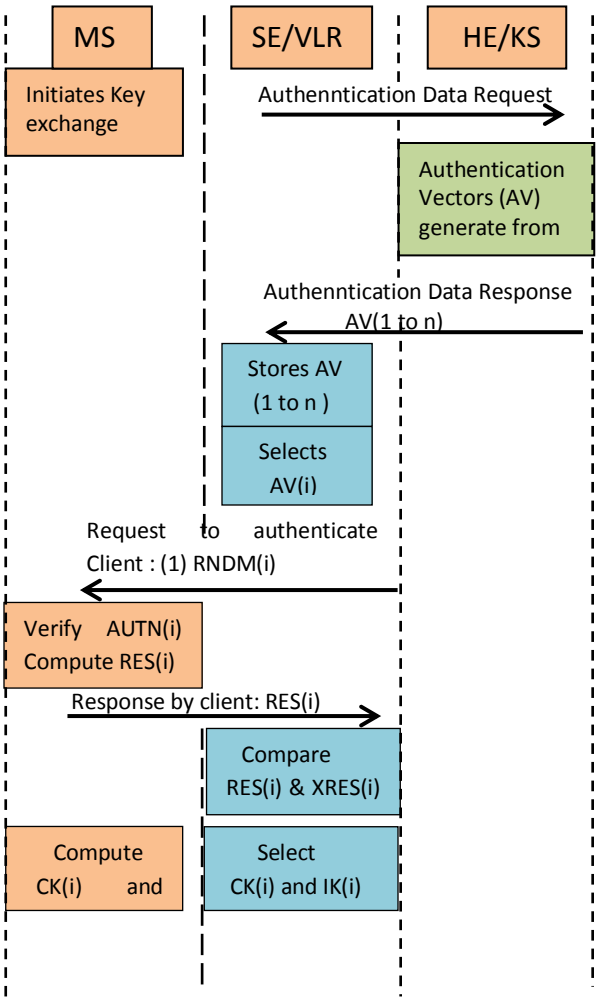


Fig 1: Architecture of UMTS AKA

The Mobile station (MS) initiates the authentication process by requesting the key server for the secret key which is not known to the Serving Network (SN). SN sends an authentication data request to the Home Environment (HE). HE responds with the authentication vector array. The authentication vector contains random number (RAND), an authentication token (AUTH), an expected response (XRES), a cipher key (CK), an integrity key (IK). SN sends a particular authentication vector and sends random number and authentication token to the Mobile Station (MS). If MS verifies the sequence number and the random number (RAND) correctly then the network is verified by the MS. MS then calculates the response (RES) using secret key and the RAND. SN compares this RES with XRES from the selected authentication vector. If RES = XRES, then MS is also verified by the network which results in the mutual authentication of both MS (client) and Network to each other [3]. A detailed description of UMTS AKA authentication process has been provided by us in [1].

III. DESCRIPTION OF 4G CORE NETWORK ARCHITECTURE

The following figure depicts the core architecture for a fourth generation network [2]. Key terms used in the figure are:

- UE(User Equipment)
- the MME (Mobility Management Entity)
- HSS(Home Subscriber Server)
- eNodeB the (the antenna)
- PCRF (Policy Charging Rules Function)
- The SGW (Serving Gateway)
- PGW (PDN(Packet Data Network) Gateway)
- A 3G access network

The User Equipment (UE) camps and chooses a certain antenna eNodeB. After choosing the suitable cell UE sends the Attach Request to the selected eNodeB through radio interface. The Attach Request contains the following parameters:

- IMSI (International Mobile Subscriber Identity)
- GUTI (Global Unique Temporary Identity)
- TAI (Tracking Area Identifier)
- PCO (Protocol Configuration Options)
- PDN type
- Ciphered Option Transfer Flag

- KSI-ASME(Key Set Identifier – Access Security Management Entity)
- NAS (Network Access Server) Sequence Number
- NAS-MAC
- P-TMSI (Packet-Temporary Mobile Subscriber Identity) signature

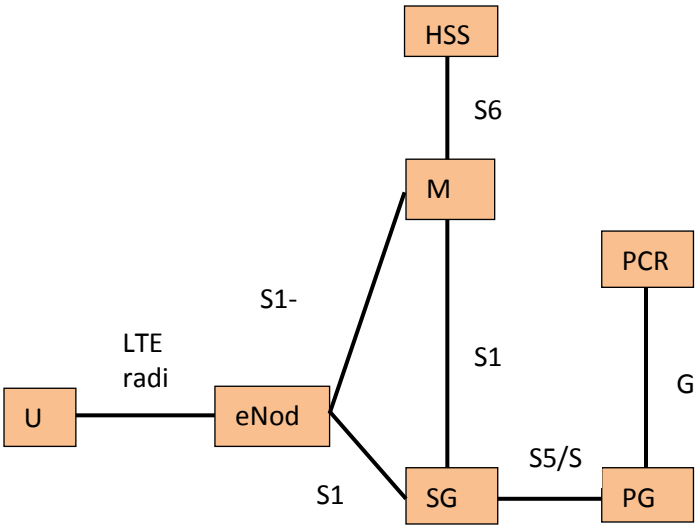
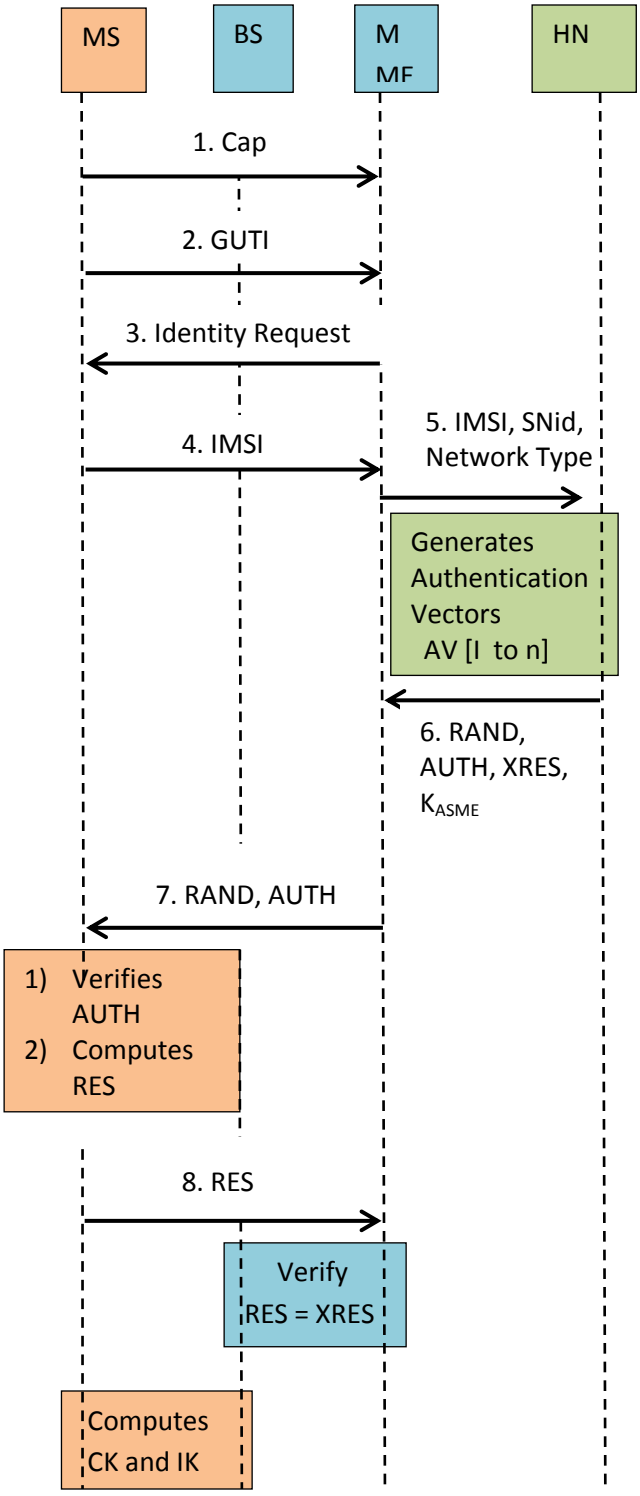


Fig 2: Architecture of 4G network.

This message is then transferred to the MME using S1-MME interface. MME uses authorizations from the HSS to validate the UE. Once the UE is verified, then an appropriate SGW is selected to access the required PLMN (Public Land Mobile Network) as requested by the UE. PLMN can also be considered as an access point by the UE. Finally the request reaches the PGW, an IP is assigned to the connection [2]. Once the IP is assigned then the connection is established between the UE and the network.

IV. ANALYZING 4G SECURITY ARCHITECTURE WITH AKA PROTOCOL

Authentication and Key agreement protocol for fourth generation network is generalized as LTE AKA. LTE AKA is built on the basis of UMTS AKA with certain improved features such as enhanced key derivation hierarchy and including Serving Network id during key derivation [1]. Certain specifications have been describes requirement for security in the proper functioning of eNodeB. Following diagram depicts the AKA operation on the 4G network architecture.



Steps involved:

Step 1: The UE sends the Attach request to the MME. MME in turn demands the IMSI number from UE if the UE is new to the area. In other case if the UE is not new in the area then the MME GUTI attached with the request to the old MME and receives IMSI from old MME in return. The IMSI along with the id of SN is then sent to the HSS.

Step2: HSS generates an array of Authentication vectors AV [1 to n]. The authentication vectors contain the following:

1) MAC = f1 (Ki, AMF, SQN, RAND).
2) XRES = f2(Ki, RAND)
3) CK = f3(Ki, RAND)
4) IK = f4(Ki, RAND)
5) AK = f5(Ki, RAND)
6) AUTN=SQN⊕AK || AMF || MAC

UMTS AKA, in LTE AKA an additional master key K_{ASME} is also derived as (K_{ASME}= KDF(CK, IK, SNid, SQN⊕AK)) along with the respective authentication vector . The derivation formula for the key proves the identity of the attached MME through SNid used. This AV[1 to n] are then sent to the MME.

Step3: MME sends the RAND and AUTH values from a particular Authentication vector selected to the MS. At MS end SQN number is verified for correct range. If SQN is in correct range then only the expected MAC is calculated and compared for the validity of the network. Once it is validated then MS calculates its RES value and sends it to the MME of BS. Calculations which take place at MS end are:

1) AK = f5(Ki, RAND)
2) SQN = 1st(AUTN)⊕AK
3) XMAC = f1(Ki, 2nd(AUTN), SQN, RAND)
4) Verify 3rd(AUTN) = XMAC
5) RES = f2(Ki, RAND)
6) CK = f3(Ki, RAND)
7) IK = f4(Ki, RAND)
8) KASME = KDF(CK, IK, SNid, 1st(AUTN))

The calculated RES is then sent over to the MME for the validation of the MS.

Step4: MME compares the RES with the XRES already present in the authentication vector. If RES = XRES, then the MS is also authenticated by BS and mutual authentication is achieved. After MS and network mutually authenticates each other, then the UE and HSS calculate CK and IK independently [1]. This is an improvement of 4G AKA over UMTS AKA such that CK and IK never leave the HSS.

CONCLUSION

In this paper first presented a detailed introduction to the basic core architecture of the 4G network and then studied the Authentication and Key Agreement protocol for LTE framework. We tried to cover the enhanced features of LTE AKA over UMTS AKA including the master key generation. As a future work, we will work to propose an enhanced LTE AKA protocol to enhance the security of 4G networks against redirection attacks.

REFERENCES

[1] C. Ttang, D.A. Naumann, and S. Wetzel, “Analysis of authentication and key establishment in Inter-generational mobile telephony”: Stevens Institute of Technology, 2013.
[2] C. Vintilă, V.V. Patriciu, I. Bica, “Security Analysis of LTE Access Network” ICN 2011, ISBN:978-1-61208-113-7.
[3] J. Kataria, A. Bansal, “Exploration of GSM and UMTS Security Architecture with Aka Protocol”, International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013, ISSN 2250-3153.
[4] A. Choudhary, R. Bhandari, “ 3GPP AKA Protocol: Simplified Authentication Process”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 12, December 2014, pp. 655-658, ISSN: 2277 128X.
[5] A. Kumar, Suman, Renu, “Comparision of 3G Wireless Networks and 4G Wireless Networks” International Journal of Electronics and Communication Engineering, Volume 6, Number 1 (2013), pp. 1-8, ISSN 0974-2166.
[6] C. Lai, H. Li, R. Lu , X. Shen, “SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks”, Computer Networks, vol.57, 2013, pp.3492–3510.
[7] L. Xiehua, W. Yongjun, “Security Enhanced Authentication and Key Agreement Protocol for LTE/SAE Network”, 978-1-4244-6252-0/11, IEEE, 2011.
[8] Third Generation Partnership Project (3GPP), 3GPP TS 33.102 v8.2.0. “3G Security; Security Architecture (Release 8),” 2009
[9] Third Generation Partnership Project (3GPP), 3GPP TS 33.401 v8.2.1. “3G System Architecture Evolution (SAE); Security Architecture (Release 8),” 2009.