Asian Journal of Electrical Sciences (AJES)
Vol.3.No.1 2015 pp18-22
available at: www.goniv.com
Paper Received :08-03-2015
Paper Accepted:20-03-2015
Paper Reviewed by: 1. R. Venkatakrishnan 2. R. Marimuthu
Editor : Prof. P.Muthukumar

AN ENHANCED AUTHENTICATION SCHEME IN HETEROGENEOUS WIRELESS NETWORK

G.GOMATHI
PG Scholar
Department of Information Technology, Adhiparasakthi Engineering College
ggomathi228@gmail.com

ABSTRACT

Heterogeneous network (HetNet) is the process of providing services to devices belonging to different evolved NodeB (eNBs) and different radio access technologies. To increase the data capacity as well as reducing the cost of all areas of network the LTE & LTE-A networks are combined and form the heterogeneous network. It also supports other radio access technology including HSPA, UMTS, EDGE, GPRS and Wi-Fi. Authentication Key Agreement (AKA) protocol is used to provide data security between nodes based on cryptography techniques. In previous papers the security is less addressed and the data's are vulnerable to active and passive attacks. In proposed system it overcomes the security issues by using existing technologies. The Enhanced Authentication and Key Agreement (EAKA) and Advanced Encryption Standard (AES(256)) encryption algorithms are used in this system.

Keywords: Heterogeneous network (HetNet), evolved NodeB (eNBs), Authentication Key Agreement (AKA),Long Term Evolution (LTE), Long Term Evolution-Advanced (LTE-A).

I INTRODUCTION

Increase in mobile data usage move the cellular wireless technology into fourth generation technology. The fourth generation Evolved packed system supports the flat IP connectivity and interworking with heterogeneous radio access networks. EPS network improves radio access technology.In the UMTS, the function of eNodeB was catagorized into NodeB and the Radio Network Controller (RNC). A LTE network includes the Evolved Packet Core (EPC) and Evolved Universal Terrestrial Radio Access Networks (E-UTRANs). An E-UTRAN has number of base stations such as eNBs, each of which communicates with user equipments (UEs) in each cell. To improve the indoor coverage and network capacity, HeNB base station is suggested by the 3GPP committee. Therefore, there are two types of the base stations existing in the LTE networks. With the growing need for mobility, when an UE moves away from the current eNB/HeNB to a new eNB/HeNB, it is indispensable to achieve a fast and stable handover in the LTE networks. LTE-Advanced are proposed to meet the requirements of International Telecommunication Union (ITU) for the fourth generation (4G) cellular systems known as International Mobile Telecommunications-Advanced (IMT-A). Among the above techniques to achieve enhancements of capacity, coverage, and spectral efficiency, an important new technique is the deployment of heterogeneous network in lte and lte-a network. After deployment of heterogeneous network the security issue is less addressed.

II RELATED WORK

Muhammad Alam.,Du Yang,Jonathan Rodriguez.,and Raed A.Abd-Alhameed[1] presents an overview of the security architecture, threads, and requirements. Based on these several solutions are given by reusing the existing security techniques. It uses the AKA protocol for providing security for user. AES encryption and Diffie hellman algorithm is used. Disadvantage in this paper is computational overhead, man in the middle attack, eaves-dropping attack. Chengzhe Lai , Hui Li,

Rongxing Lu , Xuemin (Sherman) Shen[2] SE-AKA cannot only provide strong security including privacy-preservation and KFS/KBS, but also provide a group authentication mechanism which can effectively

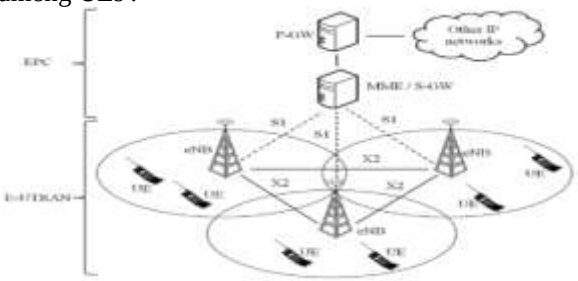
authenticate group devices. The public-key system provide mutual authentication between UE-MME and MME-HSS in the core network. The privacy for User Identification is protected and also the link in core network. The secret key is stored in USIM/MME/HSS. Mun, H., Han, K., & Kim, K [3] provide solution for 3G/WLAN system that can be extrapolated to 4G systems. It gives perfect forward secrecy, protect the user privacy and it avoids man in the middle attack. It uses the Elliptic curve cryptography and diffie-Hellman algorithm. It does not use the centralized system for EAP-AKA model. It reduces the computational overhead. Vintila, C., & Patriciu, V. [4] improves the AKA protocol by using J-PAKE mechanism to increase the strength of EPS-AKA. It overcomes lack of identification privacy. C. Koner, Member, IACSIT, P. K. Bhattacharjee[5] 3G mobile communication works on two different switching techniques. One is circuit switching for voice and low speed data communications.

The other one is packet switching mainly for data communication, but can afford voice communication like VoIP (Voice Over Internet Protocol), video telephony, multimedia service etc. It is seen that wireless communication is enhanced in packet switching technology, as a result high speed secured data as well as voice transmission-reception is possible. The future work is to invent new efficient mutual authentication technique using entities like Password, Identifier, Certified Authority, Biometric Property etc. Jacques Bou Abdo , Jacques Demerjian and Hakima Chaouchi[6] different existing EPS-EPS AKA protocols will be compared with the proposed protocol EC-AKA (Ensure Confidentiality Authentication and Key Agreement) based on security, cost effectiveness, signaling overhead, delay and performance. It is proven that EC-AKA is the exclusive protocol satisfying the New Generation Network's KPIs and it will be promoted as the target generic AKA protocol in heterogeneous networks. UMTS (Universal Mobile Telecommunications System) and GSM (Global Systems for Mobile Communications) are combined in this system.

III LTE/ LTE-A ARCHITECTURE:

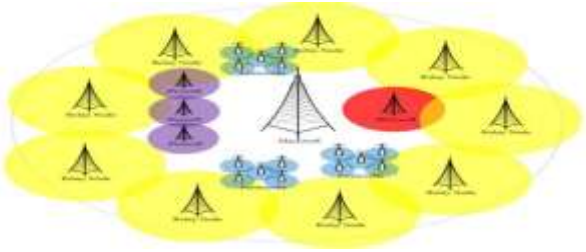
System Architecture Evolution (SAE) consists of a core network and a radio access network. The core of the network is also called as Evolved Packet Core (EPC).The EPC consist of the serving gateway (S-GW), the mobility management entity

(MME) and the packet data network gateway (P-GW). The radio access network is known as the Evolved-Universal Terrestrial Radio Access Network (E-UTRAN), which comprises user equipment (UE) and macrocell BSs. Connections between the EPC and E-UTRAN are established through the S1 interface between the S-GW and eNBs. The eNB manages transmit and receive transmissions among UEs .



HETEROGENEOUS LTE/LTE-A ARCHITECTURE:

An heterogeneous network consist of small cells such as microcells, picocells, femtocells. This results in saving the cost of deploying additional eNBs. Home evolved NodeB (HeNB) is a short-range BS with low transmission power. It utilizing a diverse set of base stations, can be deployed to improve spectral efficiency per unit area. In a homogeneous network, the strongest signal strength only served by the base stations other signals are considered as unwanted signals received from other eNBs are usually treated as interference.



IV EXISTING SYSTEM

Enable device to device communication in LTE-Advanced network. It provide solutions by reusing the existing security mechanism. It uses encryption and integrity, encryption to protect communication against eavesdropping and integrity is used to protect against

active attack. AES encryption algorithm is used(128-bit). For Key management Diffie Hellman key exchange mechanism is used. AES encryption uses this key to encrypt in source node and the same key is used to

decrypt the message in receiver side.

DISADVANTAGES OF EXISTING SYSTEM

- computational overhead
- man in the middle attack
- eavesdropping attack

V PROPOSED SYSTEM

This system combines two different radio access technologies such as Long Term Evolution (LTE) and Long Term Evolution-Advanced (LTE-A).By combining these two technologies the speed of the data transmission is increased but the security issues arises. To avoid the security problem, this system proposes solution based on applying already existing cryptographic technologies. There are two algorithms are used namely Advanced Encryption Standard and Enhanced Authentication and Key agreement.

Network access security:

• UE: It has a unique identity of user .

• UICC: The universal integrated circuit card ie., SIM card.

• eNB/RN: The evolved NodeB and relay node.

• MME:It is responsible for managing mobile location.

•HSS: This is the home subscriber server, like authentication center (AuC) ,it maintain database about the subscribers unique id, including IMEI, IMSI, and private key. LTE-A derives a group of hierarchical keys using key deviation functions (KDFs).

FEATURES

- Type
- Length
- Lifetime
- Randomization

ADVANTAGES:

- Fast data transmission
- Secure and scalable
- Prevent active and passive attack

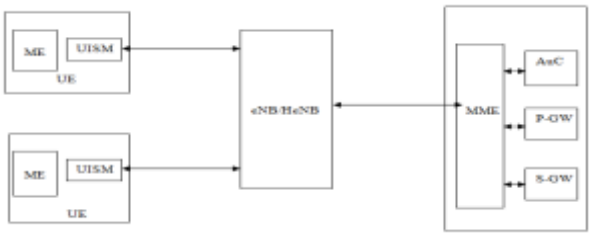
ENHANCED AUTHENTICATION AND KEY AGREEMENT

The process of authentication and key agreement (AKA) is made up of the following steps:

AUTHENTICATION AND KEY AGREEMENT:

Step 1: A user 1 sends request to MME via eNB.

Step 2:The MME sends an authentication request to Authentication Center(AuC).



Step 3:AuC sends an Authentication Vector(AV) to MME.

Step 4:MME stores the key and response, sends RAND and AUTN.

Step 5:UE compares the received AUTN and regenerated AUTN, if it matches then send response to MME.

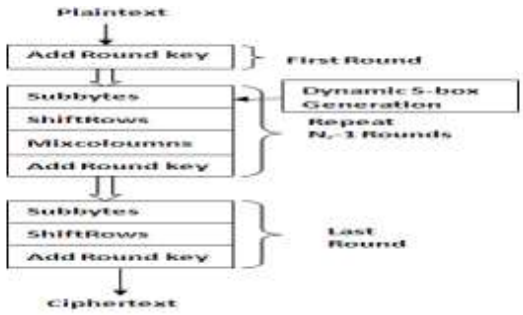
Step 6: The MME compares the stored RES to AuC RES to the received RES. If they are the same, it confirms the identity of this UE device.

AES ENCRYPTION

A 256 bits key length and 256 bit input data is given to the enhanced AES system. The proposed system's encryption and decryption is the same as traditional AES algorithm. The round function of encryption process is also similar as the traditional AES algorithm. The various models for developing enhanced system are as follows:

DYNAMIC S-BOX GENERATION

There is additional phase of making S-box dynamic as shown in Figure below. The hexadecimal digits of AES key are XOR-ed with each other and number generated by random number generator is used as the shift value to the S-box. The S-box is rotated by that shift value produced in XOR function. Before substitute byte stage, the static S-box is converted into dynamic S-box using cipher key. The inverse S-box is also modified after S-box to obtain correct inverse values.



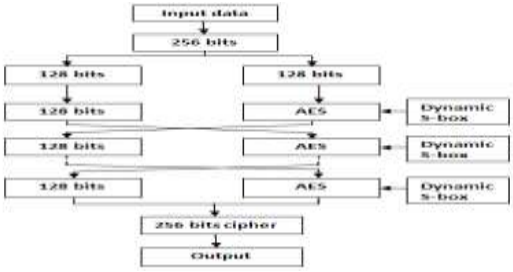
VI ROUND AES GENERATION

The Round structure of AES is used as shown in Fig.

below. Here the Input is split into two blocks of 128 bits each. One Block is given as Input to the AES section of the System. The other Block is given as Input to the AES section of the System in the next round as per the Round structure. This is done for all ten rounds respectively. These outputs are then combined together to form 256 bit block of encrypted data.

ROUND AES WITH DYNAMIC S-BOX GENERATION

Dynamic S-box is applied to the Round structure of AES as shown in below. In the round structure, ten times AES is applied to the block of data hence total ten times different S-box is created hence it is called dynamic S-box.



First the authentication is performed to check the identity of entities. If both entities are legitimate user then they are allowed for data transfer. To avoid the attacks in data processing the encryption techniques are used. For encryption there are two types of mechanism are available.Namely symmetric encryption technique and asymmetric encryption technique. In this paper symmetric encryption ie., AES is used to provide data security. This processes are worked together then this type of communication is called as secure communication. In previous paper the security is proposed for homogeneous and heterogeneous network(1^{st} -4^{th} generation) .For increasing the indoor coverage the LTE and LTE-A networks are combined. But there is a need to provide security in this heterogeneous network. This paper propose the security for heterogeneous network.

SIMULATION RESULT

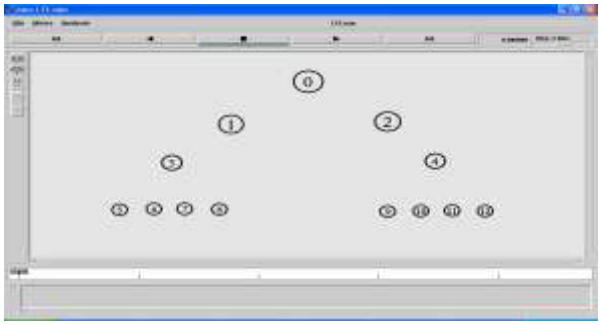
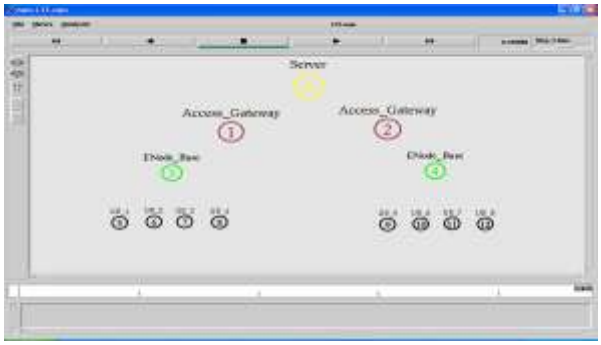


Fig a(node creation in lte network



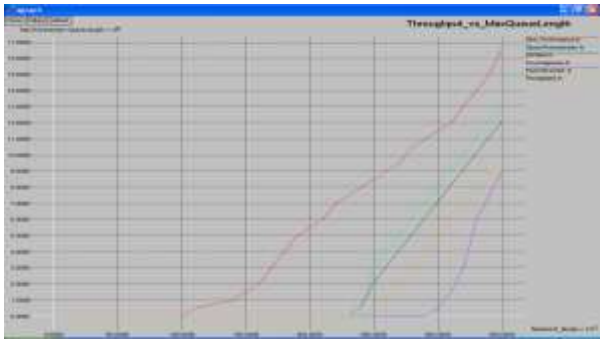


Fig b(data transmission)

VII CONCLUSION

In previous paper the security is proposed for homogeneous and heterogeneous network(1^{st} -4^{th} generation). For increasing the indoor coverage the LTE and LTE-A networks are combined. But there is a need to provide security in heterogeneous network. This paper

propose the security for heterogeneous network. The

throughput is increased and delay is minimized because the authentication and encryption uses less time to compute. This is an efficient mechanism to provide secure communication between mobile entities.

REFERENCES

[1] G. Fodor et al., "Design Aspects of Network Assisted Device-to-Device Communications,"IEEE Commun. Mag., vol. 50, no. 3, Mar. 2012, pp. 170–77.

[2] P. Phunchongharn, E. Hossain, and D. I.Kim,"Resource Allocation for Device-to-Device Communications Underlaying LTE-Advanced Networks," IEEE Wireless Commun., vol. 20, no. 4, Aug. 2013, pp. 91–100.

[3] Vintila, C., & Patriciu, V." Security Analysis of LTE Access Network". ICN 2011, The Tenth International, (c), 29-34. (2011).

[4] Muhammad Alam.,Du Yang,Jonathan Rodriguez.,and Raed A.Abd-Alhameed, "Secure Device to Device communication in LTE-A Network".IEEE.(2014).

[5] Mun, H., Han, K., & Kim, K. "3G-WLAN interworking: security analysis and new authentication and key agreement based on EAP-AKA". Wireless Telecommunications Symposium. WTS2009 (pp. 18). IEEE. (2009).

[6]J. Cao, M. Ma and H. Li, "A survey on security aspects for LTE and LTE-A networks", Communications Surveys & Tutorials, vol. 16, no. 1, (2013).

[7]A.Ghosh, R. Ratasuk, B. Mondal, N.angalvedheand T.Thomas,"LTE-advanced:Next-generation Wireless Broadband Technology", IEEE Wireless Commun., vol. 17, no. 3, (2010).

[8] Y. Park and T. Park, "A Survey of Security Threats on 4G Networks", Proc. IEEE Globecom Workshops, (2007) November.

[9]D. Forsberg, "LTE Key Management Analysis with Session Keys Context", Computer Communications, vol.33, no. 16, (2010).

[10] M. Zhang and Y. Fang, "Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol," IEEE Trans.WirelessCommun., Vol.4, No.2, Mar. 2005, pp. 734- 742. [11] M. Purkhiabani and A. Salahi, "Enhanced Authentication and KeyAgreement Procedure of Next Generation Evolved Mobile Networks,"Proc. IEEE 3rd International Conference on CommunicationSoftware and Networks (ICCSN), May 2011, pp.557-563.

[12] F. Hao and P. Ryan, J-PAKE: Authenticated Key Exchange withoutPKI," Trans. Computational Science XI, LNCS, Vol. 6480, 2010, pp.192-206. [13] Jin Cao, Maode Ma, and Hui Li, "A Group-based Authentication andKeyAgreement for MTC in LTE Networks", Proc. IEEE GLOBECOM2012, Dec. 2012, accepted for publication.