INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue6)
Available online at www.ijariit.com

Privacy Protection and Authentication Handover in 4G Network: A Survey of Literature

V. B Magalakshmi
P. G Scholar,
Department of Computer Science and Engineering,
Hindusthan College of Engineering and Technology,
Coimbatore
maha99527@gmail.com

D. Satheesh Kumar
Assistant Professor,
Department of Computer Science and Engineering.
Hindusthan College of Engineering and Technology,
Coimbatore
hicetsatheesh@gmail.com

Abstract: the 4G network is the highly advanced wireless network which aids broadband as well as multimedia applications. LTE is mainly influenced by high data rates, minimum delay and the capacity due to scalable bandwidth and its flexibility. With the rapid and widespread use LTE networks, and increase the use in data/video transmission and Internet applications in general, accordingly, the challenges of securing and speeding up data communication in such networks is also increased. A number of approaches are used for the privacy and secure data transmission on the 4G network. It also includes various algorithm and methods.

Keywords: 4G Networks, Privacy, Handover Mechanism.

I. INTRODUCTION

The Third Generation Partnership Project (3GPP) started in November 2004 to define the long-term evolution of the Universal Mobile Telephone System (UMTS) which was also one of the 3GPP projects [2]. 4G provides better data rates when compared with 2G and 3G standards due to its effective technology and standard utilized. The fourth generation of wireless standards for cellular systems is 4G, the planned successor to the 3G standard. The ITU (International Telecommunications Union) has specified that the peak speed requirements for the 4G standard are to be 100Mbps for a mobile connection (such as in a car) and 1Gbps for stationary connections (such as sitting at a computer). The 4G service is set to offer a fast and secure all-IP, roaming mobile broadband solution to devices such as laptops with wireless 4G modems, 4G smartphone mobile phones and other 4G mobile devices that require internet access with speed intensive facilities being made available, including on-demand HD television, IP telephony, on-demand gaming and, of course, high speed internet access.

1.1 4G NETWORK ARCHITECTURE

LTE is a standard for wireless data communications technology and an evolution of the GSM/UMTS standard. The main goals of LTE are to increase the capacity and data rates of wireless data networks, improve spectrum efficiency, and improve coverage, reduced latency and packet-optimized system that support multiple Radio Access. Thus, in order to achieve the goals,

the architecture of the network if different from the previous wireless data transfer network, GPRS. So, in the post, a comprehensive overview of the network architecture and basic working principle of LTE network is going to be discussed.

Basically, the LTE standard only supports packet switching with its all-IP network. The reason why LTE is designed only for packet switching is that it aims to provide seamless Internet Protocol (IP) connectivity between user equipment (UE) and the packet data network (PDN), without any disruption to the end users' applications during mobility. Due to this characteristic, voice calls and text message natively (which are typically handled by circuit-switched networks like GSM and CDMA). In LTE architecture, Evolved UTRAN (E-UTRAN) is an important role which is the air interface of LTE upgrade path for mobile networks meanwhile it is accompanied by an evolution of the non-radio aspects under the term "System Architecture Evolution" (SAE), which includes the Evolved Packet Core (EPC) network. Together LTE and SAE comprise the Evolved Packet System (EPS). Besides that, LTE network uses an eNodeB (evolved node B, essentially an LTE base station), an MME (Mobile management entity), an HSS (home subscriber server), an SGW (serving gateway), and a PGW (a packet data network gateway). These are considered as part of the EPC except eNodeB.

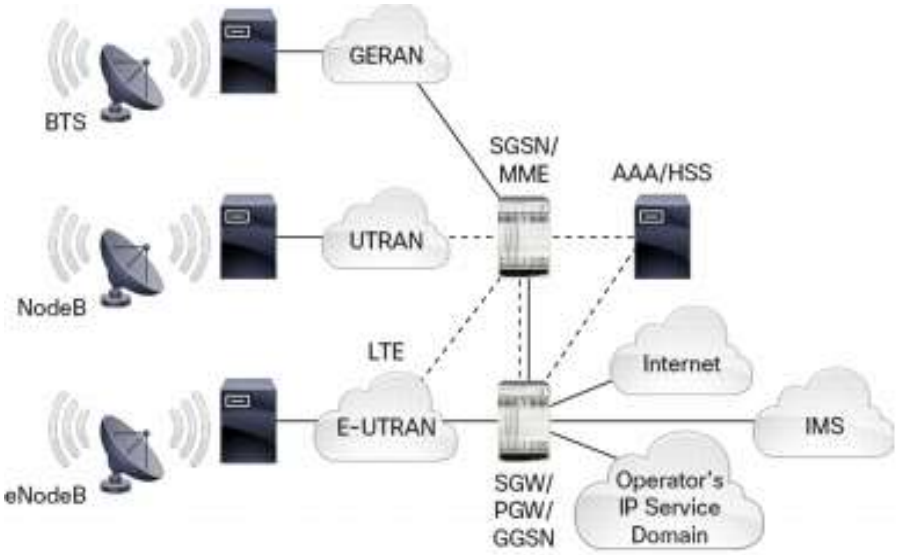

Fig 1: 4G Network.

1.2 CHALLENGES IN 4G

- Security
- Handoff Delay
- 4G supportive devices showing less Battery Backup
- Multimode Software Application
- Video Network Coding for 4G Wireless networks

1.2.1 Security

The first step in analyzing cellular wireless security is to identify the security objectives. The goals that the security policy and corresponding technology should achieve are to ensure that information generated by or relating to a user is adequately protected against misuse or misappropriation. It is to be ensured that the level of protection afforded to users and providers of services is considered to be better than that provided in contemporary fixed and mobile networks. Further, it is to be seen that the implementation of security features and mechanisms can be extended and enhanced as required by new threats and services.

1.2.2 Handoff Delay

Handoff delay poses another important QoS-related issue in 4G wireless networks. During the handoff process, the user may experience a significant drop in QoS that will affect the performance of both upper-layer protocols and applications. Deploying a priority-based algorithm and using location-aware adaptive applications can reduce both handoff delay and QoS variability. When there is a potential for considerable variation between senders' and receivers' device capabilities, deploying a receiver-specific filter in part of the network close to the
the source can effectively reduce the amount of traffic and processing, perhaps satisfying other users' QoS needs.

1.2.3 4G supportive devices showing less Battery Backup:

In 4G supportive Devices due to the presence of a large number of Transmitters & Receivers, the battery of the device runs off quite quickly. With technological developments, the devices are getting smaller in size due to Large Scale Integration and microarchitecture. Hence in 4G devices if we want to enhance the battery life by designing a much powerful Lion Battery, then the backup would increase no doubt but also the size of the device would increase i.e. not highly recommended.

1.2.4 Multimode Software Application

4G technology has a unique application of accessing several wireless networks. It is capable of high level of customization at the user-level end. This feature integrates the infrastructure of all available networks and steadily it will be easier for users to access services and applications regardless of the environment. One can easily access different mobile and wireless networks simultaneously. The multimode software is a software that allows the user device to adapt itself to various wireless interfaces networks in order to provide constant net access with high data (packet based) rate. All the networks will be compatible once the switch is completed, eliminating roaming and areas where only one type of phone is supported. Once the voice and data networks are superposed there will suddenly be millions of new devices on the network cloud. This will require either reconstruction of the address space for the entire Internet or use different address spaces for the existing wireless networks. The multimode device architecture may improve call completion and expand effective coverage area.

1.2.5 Video Network Coding for 4G Wireless networks

High Definition (HD) demand is increasing day by day more than that of the bandwidth support available. Network Coding allows reducing the required number of packets to complete a transmission over noisy or unreliable networks compared non coded version, hence increasing throughput. Network coding offers exciting possibilities for the efficient transmission of video over wireless and bottleneck networks. By sending combinations of packets and considering traffic as algebraic information not just bits, the 4G network is ideally suited to Network Coding i.e. they are resources, need to serve a variety of different devices and femto cells connected to WIFI. However, it is also noted that the complexities that Network Coding can face in decoding nodes can accelerate the capabilities of embedded systems. This problem can be discarded by use of codes defined on small Galois Fields (GF). Thus, it is inferred that Network Coding could be doing peer to peer high definition video streaming and also thereby can be incorporated into more consumer-oriented devices. In the next section, the proposed strategy for VideoCentric Network Coding has been briefly portrayed.

II. THE LITERATURE SURVEY

In this section, we discuss the various privacy protection methods as shown in table 1.

Table 1 Fingerprint Recognition method

S. No	Title	Process	Future work
1	Authentication Handover and Privacy Protection in 5G HetNets Using	The main objective of this paper is to simplify authentication handover by the global management of 5G	Due to upcoming multi-tier architecture and small cell deployment, challenges emerge in

	Software-Defined Networking[1]	HetNets through sharing of user-dependent security context information among related access points.	security provisioning and privacy protection in 5G heterogeneous networks.
2	An Efficient Authentication and Key Agreement Protocol for 4G (LTE) Networks[2]	In this paper, an Efficient EPS-AKA protocol (EEPS-AKA) is proposed thus it is based on the Simple Password Exponential Key Exchange (SPEKE) protocol.	Designing an analytical model for the proposed method to prove its efficiency.
3	Distributed Security Architecture for Authentication in 4G Networks[3]	In this paper proposed architecture, the Elliptic Curve Diffie–Hellman (ECDH) protocol is used for authenticating the mobile nodes within the network through hop by hop authentication and neighbour authentication.	Whenever a new MN enters the network then the network must initiate the process initially from the BS communicates with it and broadcasts the new MN information in the network. So, all the MN in the network record the new MN details and authenticates it.
4	GBS-AKA: Group-based Secure Authentication and Key Agreement for M2M in 4G Network[4]	This paper proposes a group-based secure authentication and key agreement (GBS-AKA) scheme, which makes our scheme to reduce the majority redundant signaling and lighten the level of congestion in the core network.	Thus the proposed the GBS-AKA scheme can reduce the higher bandwidth required during authentication. When a large number of devices visit the core network. It Could withstand only for some extent. It has to be rectified in the future work
5	Authentication of Nodes among Different Symmetric Key Groups in MANETs using 4G Technologies[5]	In this paper, a scheme is introduced were the nodes having common interests, once authenticated through external resources, form a group with a single key shared by the whole group.	The scheme can be regarded as an optimized extension of the Tseng and pair-wise symmetric key models.If nodes do not possess a common interest this scheme cannot be implemented.
6	Enhanced user Security and Privacy Protection in 4G LTE Network[6]	This paper proposes a change to the EPS-AKA authentication process in 4G Long Term Evolution (LTE) Network by including the use of Public Key Infrastructure (PKI). The change would result in the IMSI never being released in the clear on an un-trusted network.	4G LTE that an attacker can take advantage of such as denial of service and paging attacks. Moreover, implementing mutual authentication between the UE's and eNB's would also assist in minimizing such security risk (DoS) in 4G LTE. This, of course, needs to be deployed in the nearest future.
7	QoS-aware Frequency-based 4G+Relative Authentication Model for Next Generation LTE and its Dependent Public Safety Networks[7]	In this paper it is proposed the 4th-Generation plus Relative Authentication Model (4G+RAM), which is composed of two dependent protocols: i) Privacy-protected Evolved Packet System Authentication and Key Agreement (PEPS-AKA) Protocol for the initial authentication and ii) 4th-Generation plus Frequency-based Re-authentication Protocol (4G+FRP) for	The proposed 4G+RAM with PEPS-AKA and 4G+FRP ensures privacy protection and seamless, secure communication in LTE and LTE-dependent future-generation PS networks.

		the re-authentication of known and frequent users.	
8	A Survey on Security Aspects for LTE and LTE-A Networks[8]	In this paper, they have overviewed the security issues in the LTE/LTE-A 4G wireless networks. It had first presented the security architectures and mechanisms specified by the 3GPP standard and also discussed the vulnerabilities existing in the security architecture of the LTE/LTE-A wireless networks and reviewed the corresponding the state-of-the-art solutions proposed to overcome those security flaws in the literature	This survey paper had explored that there are still a lot of security issues in the current LTE/LTE-A networks and it could be resolved in the future works.
9	Security Advances and Challenges in 4G Wireless Networks[9]	This paper presents a study of security advances and challenges associated with emergent 4G wireless technologies. The security-related standards, architecture, and design for the LTE and WiMAX technologies are analyzed and security issues, vulnerabilities present in the above 4G standards are discussed.	It is suggested that there is a critical need to augment this initial research with emulation and testbed related studies which will likely reveal further issues and challenges to be addressed.
10	Security Scheme For 4G wireless Systems[10]	In this paper security policy including authentication, authorization, account, and audit (AAAA) is discussed according to the features of 4G systems. Meanwhile, the security architecture scenario based on hybrid PKI trust model and mobile IPv6 is proposed. Over this architecture a novel hybrid authentication and key agreement scheme that associate's dynamic password with public-key mechanism is presented to provide lightweight authentication and non-repudiation service.	The key management is more convenient and feasible since ME doesn't need to hold a public-key certificate. So, the scheme suggested in this paper is convenient to support global mobility and flexible scalability with low computational power and secure communication. Accordingly, it is very suitable for 4G mobile communication systems.

CONCLUSION

In this paper, we have discussed various privacy protection and authentication mechanism algorithms and methods which can be used for security and authentication in 4G networks. These mentioned methods conclude that there are lots of algorithms and techniques used in 4G networks for security and it also needs lots of improvisation due to enabling technology.

REFERENCE

[1] X. Duan and X. Wang, "Authentication handover and privacy protection in 5G hetnets using software-defined networking," IEEE Communications Magazine, vol. 53, no. 4, pp. 28–35, Apr. 2015.

[2] K. A. Alezabi, F. Hashim, S. J. Hashim, and B. M. Ali, "An efficient authentication and key agreement protocol for 4G (LTE) networks," in 2014 IEEE REGION 10 SYMPOSIUM, 2014.

[3] D. Niranjani and M. G. Durga, "Distributed security architecture for authentication in 4G networks," in 2016 IEEE International Conference on Advances in Computer Applications (ICACA), 2016.

[4] J. Yao, T. Wang, M. Chen, L. Wang, and G. Chen, "GBS-AKA: Group-Based Secure Authentication and Key Agreement for M2M in 4G Network," in 2016 International Conference on Cloud Computing Research and Innovations (ICCCRI), 2016.

[5] A. I. Sheikh, W. Noshairwan, M. Rashid, S. M. Gilani, E. Irshad, and M. Usman, "Authentication of Nodes among Different Symmetric Key Groups in MANETs Using 4G Technologies," in 2009 International Conference on Computer Engineering and Technology, 2009.

[6] O. E. Ekene, R. Ruhl, and P. Zavarsky, "Enhanced User Security and Privacy Protection in 4G LTE Network," in 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), 2016.

[7] S. B. M. Baskaran, G. Raja, A. K. Bashir, and M. Murata, "QoS-aware Frequency-based 4G+Relative Authentication Model for Next Generation LTE and its Dependent Public Safety Networks," IEEE Access, pp. 1–1, 2017.

[8] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A Survey on Security Aspects for LTE and LTE-A Networks," IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 283–302, 2014.

[9] N. Seddigh, B. Nandy, R. Makkar, and J. F. Beaumont, "Security advances and challenges in 4G wireless networks," in 2010 Eighth International Conference on Privacy, Security, and Trust, 2010.

[10] Yu Zheng, Dake He, LixingXu, and Xiaohu Tang, "Security scheme for 4G wireless systems," in Proceedings. 2005 International Conference on Communications, Circuits and Systems, 2005.

