Comparative study and Security Limitations of 4G Network

(Case Study LTE and WIMAX)

Chukwu Michael .C

chukwu.michael@cstd.nasrda.gov.ng

***Abstract*--The advancement and migration of the broadband wireless communication technology into the next generation technology known as Fourth Generation (4G) network has indeed become the next emergent wireless revolution, as an important milestone beyond third generation. Long-Term Evolution (LTE) and Worldwide Interoperability for Microwave Access (Wimax) are among the numerous new innovation technologies which have evolved as leading contenders for the 4G technology. The high speed capability and wider coverage has been a good achievement for 4G networks. Nevertheless, security and improved higher speed with a better quality of service (QOS) has been an issue in its network operations due to the open nature and all IP infrastructure of 4G network. This paper explores the trends in the evolution of 4G wireless technology and its security limitations. It studies the wireless standards of 4G technologies. Also, the security related architecture for the LTE and Wimax technologies are analysed. Finally, it evaluates and recommends ways of tackling the security issues in 4G network.**

Keywords: Security, 4G Wireless, LTE, Wimax.

I. INTRODUCTION

The next generation of wireless communication technology known as fourth generation (4G) allows operators to use new and wider spectrum and supplements third generation 3G and 3.5G wireless technologies with higher user data rates, lower latency and a complete internet protocol(IP) base network architecture[6].Long Term Evolution (LTE) and (Worldwide interoperability for Microwave Access) are the two wireless technologies that have been considered as aspirants to achieve the 4G wireless performance objectives, due to their high speed capability, strong quality of service(QOS) and wider coverage. There are number of differences between the 4G wireless when compared with 3G and other earlier technologies .The major difference is the fact that 4G wireless network operates entirely on the IP protocol and architecture, which is what brought about the similarity between LTE and Wimax. However, these two technologies also differ from each other in some other aspects such as network architecture and security. Consequently, the open nature and all IP base infrastructure of these 4G wireless networks have increase security issues when compared with other wireless technologies and also significant attention has been given to security design during the development of both the LTE and Wimax standards.

The mission of securing 4G wireless networks and systems is a very challenging one owning that a lot of sacrifice must be made each time extra security mechanisms are carried out in its network as an IP based network, there is an impact on the performance and traffic handling capacity of the network and quality of service. The purpose of this paper is to investigate the evolution of 4G technology and its security limitations and challenges, this aim at identifying areas which need further attention. This will focus mostly on specific MAC layer security issues that are distinctive to LTE & Wimax. Secondly, the standardization of 4G wireless network and the evaluation of the network architecture will be analysed and its security evolution will be discussed.

II. 4G NETWORK STANDARDS

The International Telecommunication Union (ITU) named the International mobile Telecommnication-2000 (IMT-2000) as a global standard for 3G wireless communications in previous time but later went further to improve the initiative by introducing IMT-Advance which is considered as the specification for 4G wireless[1]. The objective of IMT Advance stated that 4G wireless technology must support the following:

1) High data rate (1Gbps peak rate for low mobility and 100Mbps peak rate for high mobility).
2) High capacity.
3) Low cost per bit.
4) Low latency.
5) Good quality of service (QOS).
6) Wider coverage.

7) Mobility support at high speeds.

Several broadband wireless access technologies have been developed but only LTE developed by 3GPP and Wimax developed by IEEE 802.16 got the characteristics for 4G wireless technology[2].

III. 4G NETWORK ARCHITECTURE

A. LTE

LTE offers high spectral efficiency, low latency and high peak date rates, it influences the economics of scale of 3G as well as ecosystem of infrastructure to provide the highest performance in a cost effective manner. The latest study being developed by 3GPP is an evolution of 3G into an evolved radio access called LTE and evolved packet access core network in the system Architecture Evolution(SAE)[3].

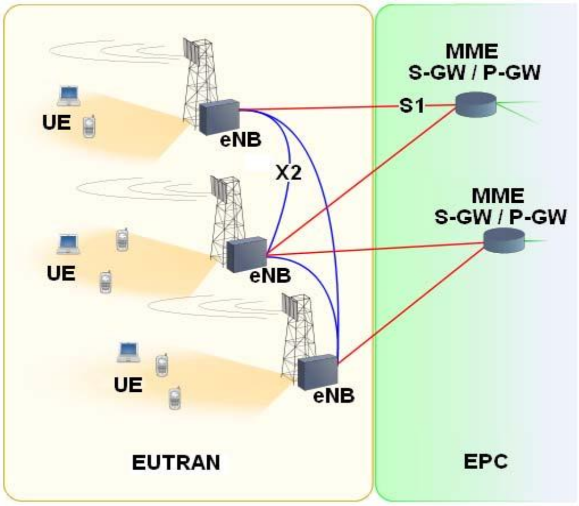

Figure 1:LTE-System Architecture Evolution(SAE)[3]

Figure 1 above shows the LTE architecture. The User equipment (UE) like mobile phone or computer connects to the wireless through the eNodeB within the E-UTRAN (Evolved UMTS Terrestrial Radio Access Network)..The E-UTRAN connects to the EPC (Evolved Packet Core) which is IP-based. The EPC connects to the provider wire line IP network. An LTE network has two types of network elements :- (i) the eNodeB which is an enhanced base station which incorporates all the radio interface-related functions for LTE. The eNodeB also carried higher functions like Inter-cell radio resource management (RRM), Radio admission control, Scheduling via dynamic resource allocation, Enforcement of negotiated QoS on Uplink and compression/decompression of packets destined to/from the UE. (ii) The Access Gateway (AGW) which comprises all the functions for the EPC. The AGW consist of multiple of modules such as Home Subscribe Server (HSS), Packet Data Network Gateway (P-GW), Serving Gateway(S-GW) and Mobility Management Entity (MME) which is the key control node responsible for managing the UE identity as well as security authentication and mobility. The LTE standard is flexible which makes it to allow the combination of these AGW modules into a single or multiple devices. LTE maintains a meshed architecture which allows greater efficiency and performance gains. For instant a single eNode can communicate with multiple Access Gateways. LTE utilizes a flat all IP-based architecture and traffic originating at a UE is generated in a native IP format and then processed by eNodeB & AGW [4]. The main task of AGW is to distribute the migration of messages to eNodeBs; security control, encryption of user data ,switching of U-plane to support UE mobility and idle mode mobility handling[5].

B. WIMAX

Figure 2 below shows the end to end network architecture of Wimax. It is made of up Access Service Network (ASN) and Connectivity Service Network (CSN) just like LTE has E-UTRAN and EPC. The ASN represents a complete set of network functions required to provide radio access to the mobile station (MS) and is decomposed into ASN gateway(ASN-GW) and Base Stations(BS). The BS includes radio functions of the ASN interfacing with the MS over air link according medium access control (MAC) and physical (PHY) layers defined in IEEE 802.16 specifications[2]. The ASN-GW represents accumulation of ASN functions that are link to QoS, security and mobility management for all connections served by BSs[8]. For CSN, it is a set of network function that provide all IP connectivity services to WIMAX subscribers.it comprises of the following network elements: (i) authentication, authorization and accounting servers (AAA) which processes controls signals form the ASN-GW to authenticate the MS. (ii)Home Agents(HA) which enable global mobility and also processes signals from ASN-GW and anchors the IP payload after assigning a mobile IP address to the MS. The HA server provides the connectivity to the internet for data traffic. For example if the MS makes a VOIP call, control is passed to the CSN IMS (IP Multimedia System) server which then process the call. If the call is to a telephone number outside Wimax network, the IMS server select the appropriate Media Gateway Controller (MGC)/Media Gateway (MGW) to interface to the Public Switch telephone Network(PSTN).The communication between the MS and BS (using air interface) is via all IP bearer and control. Like LTE which is an all-IP flat network, Wimax doesn’t have a TDM (Time Division Multiplexing)bearer[4].

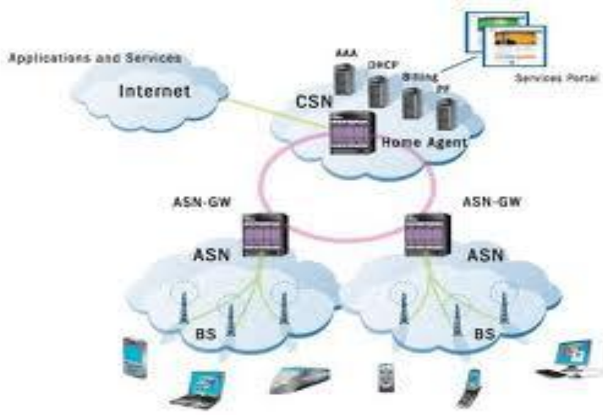

Figure 2: Mobile Wimax Network Architecture[6]

IV. EVOLUTION OF SECURITY IN 4G NETWORK.

In 4G wireless network, security is a very important issue and the security requirements are in these main aspect: (i) the users that want to use the network must be authenticated. (ii) the device that will be connected to the network must be authenticated. To meet these two main requirements, security credentials, usually include identity, certificates, username and password, are to be required for authentication. To authenticate these credentials, security infrastructures like AD server and CA are usually deployed and develop as service[1].

A. *Security Evolution in LTE*

In cellular networks, the security architecture evolved in continuation lane. In first generation wireless, hackers could snoop in conversation over the network and also could gain full access to the network [1]. In GSM (2G), authentication algorithms were not very strong. Just with little interaction with a SIM card (subscriber identity module) could show the master security key[6] In UMTS (3G) wireless, the authentication mechanism was improved to a two-way process. Both the network and the mobile user used encryption and integrity keys to create stronger security. Also, some mechanisms were introduced to ensure freshness of the integrity keys. Which means if a key is broken ,the damage will only last for a little period of time that is the validity of the key will last just a short time then goes invalid[3]

In LTE (4G), just like UMTS’s transition from 2G, further improvements were introduced. For instance , In 2G, a solitary unique ID was used on the SIM card, in 3G and subsequently 4G LTE, temporary ID and further abstraction was used so that there will be little or no opportunity of intruder to steal identities. Another mechanism to strengthen security in 4G was to add secure signalling between the UE and MME (Mobile Management Entity). Finally security measures were put in place for interworking between 3GPP and trusted non 3GPP users [7].

The evolution and transition from 1G to 4G witnessed significant security protection. However, analysis indicates that the dual manifestation of operating an open IP-based architecture as well as the complexity of security hackers means that security issues remain a matter of key concern in 4G network systems. Serious attention need to be given to analysing security challenges in 4G wireless and rapid development of solutions for threat detection and extenuation[8]

1. *LTE Security Model*

The figure below shows the authentication method of LTE with step by step details[1]:

a. The authentication process starts by the authentication server sending EAP (Enhance Authentication Protocol)-Request /Identity message to the supplicant or User Equipment (UE).
b. The supplicant responses by replying the EAP-response/Identity message containing the identity message and NAI(Network Access Identifier).
c. Upon receipt of the EAP-response/identity message , the authentication server retrieves the supplicant’s certificate from the certificate repository.

d. The authentication server generates the EAP-Request/AKA-Challenge message using the standard AKA way.

e. The authentication server sends the EAP-Request/AKA-Challenge message encrypted by the supplicant's public key to the supplicant.

f. The supplicant decrypts the EAP-Request/AKA-Challenge message using its own private key.

g. The supplicant sends the EAP-Response/AKA- Challenge to the authentication server.

h. The authentication server decrypts the information using server's private key and verifies the EAP-response/AKA-Challenge message using AKA algorithm.

i. If the message is correct, the EAP server sends the EAP success message to the Supplicant.

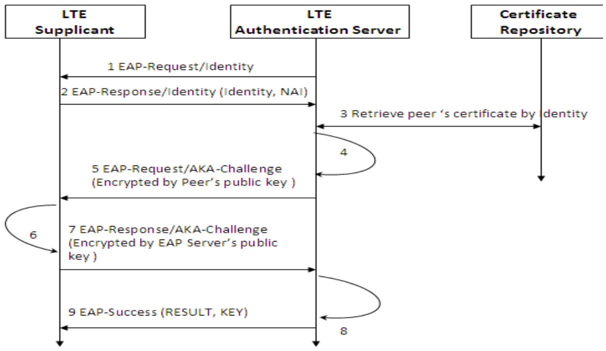
LTE Supplicant
LTE Authentication Server
Certificate Repository
1 EAP-Request/Identity
2 EAP-Response/Identity (Identity, NAI)
3 Retrieve peer 's certificate by identity
4
5 EAP-Request/AKA-Challenge (Encrypted by Peer's public key)
6
7 EAP-Response/AKA-Challenge (Encrypted by EAP Server's public key)
8
9 EAP-Success (RESULT, KEY)

Figure 3: Enhanced LTE Authentication process [1]

B. Security Evolution in Wimax

The IEEE 802.11 security issues were incorporated by the Wimax group into IEEE 802.16 standards. It is stated that as Wimax standard evolved from 802.16 to 802.16a to 802.16e, the requirement evolved from the line of sight to mobile Wimax. The security requirements and standards also evolved to address the changing demands.

The security features of the initial IEEE 802.16 standard to enhance the IEEE 802.16e standard. The key new features are listed as follows: (i) Privacy Key Management Version2 (PKMv2) protocol. (ii) User authentication is carried out using Extensible Authentication Protocol(EAP) method (iii)Message authentication is done using Hash-based Message Authentication Code(HMAC) or Cipher-based Message Authentication Code (CMAC) scheme (iv) confidentiality is achieved using Advance Encryption Standards(AES)[9]

In spite of this, the strength of security of 802.16e still requires much more improvements as it is transiting to 802.16m standard. Over-the-air security remains a key part of ensuring end-to-end network security in WIMAX. While security architecture have been developed to mitigate against threats over-the-air, there are still a number of associated challenges. An analysis shows that the main challenge will be to balance security needs with the cost of implementation, performance and interoperability. Since Wimax uses IP transport mechanism in handling control /signalling and management traffic, network operators will have to defend against general IP security threats as well[4]

2. *WIMAX Security Model*

Wimax standards defines medium access control(MAC) for communication between the base station and the mobile station, which consists of the authentication, authorization and accounting (AAA), key management and encryption. The Wimax can use any of these Extensive Authentication Protocol (EAP)-authentication scheme; Transport Layer Security (EAP_TLS) and Transport Tunnelled Layer Security (EAP_TTLS) protocol to do authentication. The EAP_TTLS protocol which is mostly used, uses its security credential to support establishment of secured connection in a roaming environment and protect user credential [1]. Figure 4 below shows the details of the authentication processes. Wimax uses privacy key management for securing key distribution and synchronization between BS and MS .Encryption comes in only when the key exchange is successful, the BS uses the authorization key (AK) to generate the Traffic Encryption Key(TEK).The TEK is utilized for secure encryption of data across the wireless link[9].

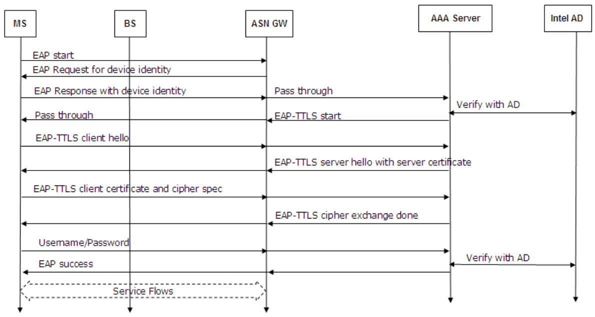
MS
BS
ASN GW
AAA Server
Intel AD
EAP start
EAP Request for device identity
EAP Response with device identity
Pass through
Verify with AD
Pass through
EAP-TTLS start
EAP-TTLS client hello
EAP-TTLS server hello with server certificate
EAP-TTLS client certificate and cipher spec
EAP-TTLS cipher exchange done
Username/Password
Verify with AD
EAP success
Service Flows

Figure 4: Wimax Authentication process[1]

V. SECURITY PROBLEMS OF 4G WIRELESS

A. LTE –MAC Layer security hitches

The best way of describing LTE security issues is to list them in collections. The major issues considered here are as follows:-(i) illegal use of user and mobile equipment identities to access network services (ii) user tracking based on the temporary user identifiers, signalling messages etc. (iii) illegal access and usage of security procedure keys to access network services (iv) malicious modification of UE parameters (e.g. failure timers, retry timers) to lock out an UE from normal services (v) wilful tampering of the eNodeB system broadcast information (vi) eavesdropping and illegal modification of IP packet contents (vii) Denial of Service attacks launched on the UE or eNodeB (viii) data integrity attacks (signalling or user data) using replay[10].

B. WIMAX –MAC Layer security hitches

The IEEE 802.16 radio interface standard describes several steps in order for a Mobile Station to establish initial access with a Base Station. These steps are (i) Scanning and Synchronization (ii) UL Parameter Acquisition (iii) Initial Ranging and Time Synchronization (iv) Basic Capabilities Negotiation (v) MS Authorization and Key Exchange (vi) Registration with the Serving BS (vii) Connection Establishment. The first five steps involve non-secure traffic. Thus, they are prone to various attacks. The last two steps involve secure traffic exchange based on the device authentication standards of Wimax. There are various sources of potential vulnerabilities in Wimax 802.16e [2 , 9 , 11]. Some of these sources include: (i) The fact that management MAC messages are never encrypted providing opponents an ability to listen to the traffic and potentially gain access to sensitive information (ii) The fact that some messages are not authenticated (no integrity protection). Typically, a hash based message authentication code (HMAC) is used as digest. However, this is not used for broadcasts and a few other messages. Simple forgery can affect communication between an MS and BS (iii) weakness in authentication and authorization procedures is an enabler for the BS or SS masquerading threat. It is not easy to get the security model correct in a mobile environment due to limited bandwidth and computation resources (iv) Issues with key management such as the size of the TEK identifier and TEK lifetime are considered as potential sources of liabilities for Wimax security[12]. There are four categories of attacks at the MAC layer of Wimax, which are listed as follows; (1) Service Degradation (2) Denial of Service (3) Authorization vulnerability and (4) key management[4]

C. PHYSICAL Layer hitches.

Both Wimax and LTE are subject to two key liabilities at the physical layer - Interference and Scrambling attacks [13]. By deliberately inserting man-made interference onto a medium, a communication system can stop functioning due to a high signal-to-noise ratio. There are two types of interference that can be carried out: (i) noise and (ii) multicarrier [12]. Noise interference can be performed using White Gaussian Noise (WGN). In the case of Multi-carrier interference, the attacker identifies carriers used by the system and injects a very narrowband signal onto those carriers.

VI. CONCLUSION

In this paper, the study of 4G network evolution and security challenges revealed that both LTE and Wimax[14] resemble each other in flat network architecture, having pure IP architecture, high capacity ,wide coverage range etc. This study explains the standards and evolution of 4G network. It analysed the network architecture of LTE and Wimax .The authentication process, security challenges and models of 4G network were discussed with more attention on the MAC layer susceptibilities for LTE and Wimax. At MAC layer Wimax is vulnerable to Denial of service attacks, service degradation and key management, while LTE also has its own set of susceptibilities which are location tracking, bandwidth stealing and denial of service. But at the physical layer, both LTE and Wimax are subject to interference and scrambling attacks which are the major problems in the physical layer. Because of the open nature of IP base 4G network, there is an increased likelihood of security attacks, and therefore, multiple levels of security including the follow; Encryption, Authentication, Authorization, frequent key refresh (Cryptanalysis) and Address concealment Increased should be applied frequently.

REFERENCES

[1] Y. Leo, M. Kai, and A. Liu, "A comparative study of WiMAX and LTE as the next generation mobile

enterprise network," in *Advanced Communication Technology (ICACT), 2011 13th International Conference on*, 2011, pp. 654-658.

[2] H. Chin-Tser and J. M. Chang, "Responding to Security Issues in WiMAX Networks," *IT Professional*, vol. 10, no. 5, pp. 15-21, 2008.

[3] G. A. Abed, M. Ismail, and K. Jumari, "Traffic Modeling of LTE Mobile Broadband Network Based on NS-2 Simulator," in *Computational Intelligence, Communication Systems and Networks (CICSyN), 2011 Third International Conference on*, 2011, pp. 120-125.

[4] N. Seddigh, B. Nandy, R. Makkar, and J. F. Beaumont, "Security advances and challenges in 4G wireless networks," in *Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on*, 2010, pp. 62-71.

[5] Z. Muxiang and F. Yuguang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," *Wireless Communications, IEEE Transactions on*, vol. 4, no. 2, pp. 734-742, 2005.

[6] M. Shin, J. Ma, A. Mishra, and W. A. Arbaugh, "Wireless Network Security and Interworking," *Proceedings of the IEEE*, vol. 94, no. 2, pp. 455-466, 2006.

[7] S. Kasera and N. Narang, *3G mobile networks : architecture, protocols and procedures : based on 3GPP specifications for UMTS WCDMA networks*. New York: McGraw-Hill, 2005.

[8] M. Sauter, *Beyond 3G : bringing networks, terminals, and the Web together : LTE, WiMAX, IMS, 4G devices and the mobile Web 2.0*. Chichester: Wiley, 2009.

[9] P. Rengaraju, L. Chung-Horng, Q. Yi, and A. Srinivasan, "Analysis on mobile WiMAX security," in *Science and Technology for Humanity (TIC-STH), 2009 IEEE Toronto International Conference*, 2009, pp. 439-444.

[10] C. B. Sankaran, "Network access security in next- generation 3GPP systems: A tutorial," *Communications Magazine, IEEE*, vol. 47, no. 2, pp. 84-91, 2009.

[11] D. Johnston and J. Walker, "Overview of IEEE 802.16 security," *Security & Privacy, IEEE*, vol. 2, no. 3, pp. 40-48, 2004.

[12] D. Pulley, "Infrastructure implementation challenges for LTE and WiMAX air interfaces," in *Hot Topics Forum: LTE vs WiMAX and Next Generation Internet, 2007 Institution of Engineering and Technology*, 2007, pp. 1-25.

[13] M. J. Chang, Z. Abichar, and H. Chau-Yun, "WiMAX or LTE: Who will Lead the Broadband Mobile Internet?," *IT Professional*, vol. 12, no. 3, pp. 26-32, 2010.

[14] L. Song, J. Shen, and Books24x7 Inc., 2011. Evolved cellular network planning and optimization for UMTS and LTE. [Online eBook]. Available: [Accessed: