SECURITY ISSUES AND LIMITATIONS OF 4G WIRELESS TECHNOLOGY SYSTEM

Mr. Prakash Kumar Lange
Department of Computer Science and Application, St. Aloysius' College, (Auto.), Jabalpur, Madhya-Pradesh, INDIA

Abstract:
Mobile Communication, Broadband technology has been developed rapidly since last few eras. The growth of the wireless broadband technologies in the modern years was the answer of increasing demand for mobile Internet and wireless multimedia application such as live TV streaming, live Movies, video conferencing, Supportive Software Applications etc. However current design practices involve to build independent networks that each make their own resource decisions. In this paper I present a clear aspects approach to explore the trends in the evolution of 4G wireless technology and its security limitations. During a common Worldwide Interoperability for Microwave Access WiMAX and LTE has facilitate convergence of mobile and fixed broadband network. The approach requires the following expectations to hold: 1) To create the independent, autonomous wireless systems (AWSs) to home and cooperate with each other to provide users with global broadband wireless coverage; 2) In the geographic area, a cell phone or Wireless supportive devices might have access to many independent, autonomous wireless networks; 3) Routers, access points and repeaters will support a small number of adaptive radios that are capable of operating in a number of supported communication modes. I am going to identify the key research challenges to be addressed to move the idea and concept to a viable, reliable and independent supportive network system.

Keywords— WiMAX, LTE (Long Time Evolution), MIMO (Multiple Input Multiple Output), heterogeneous wireless networks.

I. INTRODUCTION

The wireless communication technologies have been attractive promptly day to day. Electronic devices continue to shorten in size and at the same time growing in processing power. Users generally insist in more sophisticated and worthwhile applications. Hence, capacity improvement is the supreme necessity in wireless communications [1]. The evolution of the mobile services starting from the 1G (first generation) to 4G (fourth generation) is begun as follows:

1G: The first generation of mobile network was deployed in Japan by Nippon Telephone and Telegraph Company (NTT) in Tokyo during 1979. In the beginning of 1980s, it gained popularity in the US, Finland, UK and Europe. This system used analogue signals and it had many disadvantages due to technology limitations.

2G: Second generation of mobile communication system introduced a new digital technology for wireless transmission also known as Global System for Mobile communication (GSM). GSM technology became the base standard for further development in wireless standards later. This standard was capable of supporting up to 14.4 to 64kbps (maximum) data rate which is sufficient for SMS and email services. Code Division Multiple Access (CDMA) system developed by Qualcomm also introduced and implemented in the mid-1990s. CDMA has more features than GSM in terms of spectral efficiency, number of users and data rate.

2.5G & 2.75G: In order to support higher data rate, general Packet Radio Service (GPRS) was introduced and successfully deployed. GPRS was capable of data rate up to 171kbps (maximum). EDGE – Enhanced Data GSM Evolution also developed to improve data rate for GSM networks. EDGE was capable to support up to 473.6kbps (maximum). Another popular technology CDMA2000 was also introduced to support higher data rate for CDMA networks. This technology has the ability to provide up to 384 kbps data rate (maximum).

3G: Third generation mobile communication started with the introduction of UMTS – Universal Mobile Terrestrial / Telecommunication Systems. UMTS has the data rate of 384kbps and it support video calling for the first time on mobile devices. After the introduction of 3G mobile communication system, smart phones became popular across the globe. Specific applications were developed for smartphones which handles multimedia chat, email, video calling, games, social media and healthcare.

4G: 4G, the fourth-generation of wireless service, is an enhancement from 3G and is presently the most extensive, widespread, expeditious and high-speed wireless service. Presently 4G is available only in limited regions. 4G wireless service has been devised to deliver high speed irrespective of the technology which drives 4G. For instance Sprint employs a technology called WiMAX for its 4G services, whereas Verizon Wireless employs Long Term Evolution, or LTE. On an average, 4G wireless technology is expected to provide data rates from four to ten times higher than today's conventional 3G networks.

II. FOURTH GENERATION NETWORKS

4G or Fourth Generation is future technology for mobile and wireless communications. It will be the successor for the 3rd Generation (3G) network technology. Currently 3G networks are under deployment. Approximately 4G deployments are expected to be seen around 2010 to 2015. There is no formal definition for what 4G is; however, there are certain objectives that are projected for 4G. These objectives include, that 4G will be fully IP based integrated system. 4G will be capable of providing between 100 Mbps and 1Gbps speeds both indoor and outdoor with premium quality and high security. The evolution from 3G to 4G will be driven by services that offer better quality (e.g. multimedia, video and sound) thanks to greater bandwidth, more sophistication in the association of a large quantity of information, and improved personalization. Convergence with other network (enterprise, fixed) services will come about through the high session data rate. Machine-to-machine Transmission will involve two basic equipment

types: sensors (which measure parameters) and tags (which are generally read/write equipment). In simplest terms, 4G will be an integrated system of voice, data and image communications that will support a wide range of personal and business communications.

The history and evolution of mobile service from the 1G (first generation) to 4G (fourth generation) are discussed in this section. As the second generation was a total replacement of the first generation networks and handsets, and the third generation was a total replacement of the second generation networks and handsets, so the fourth generation cannot be just an incremental evolution of 3G technologies. The following table presents a short history of mobile telephone technologies.

III. FEATURES OF 4G

1) A spectrally efficient system
2) High network capacity i.e. more simultaneous users per cell
3) A nominal data rate of 100 Mbps while the client physically moves at high speed relative to station, and 1Gbps while client and station are in relatively fixed positions as defined by ITU
4) Smooth handoff across heterogeneous networks, seamless connectivity and global roaming across multiple networks
5) High quality of service for next generation multimedia support (real time audio, high speed data, HDTV video content, mobile TV, etc.)
6) Global mobile access (terminal and personal mobility)
7) High quality of service (full coverage, intelligibility, no drop, and no/lower call blocking and latency)
8) Easy and simple access to multimedia voice, data, message, video, Worldwide Web, Global Positioning System (GPS), etc.
9) Power efficiency- 100 MOPS/mW and more
10) High-level modem virtual machine interface (VMI), simplified programming for each standard, enhanced reuse across standards
11) Integration across many platforms, no digital signal processing (DSP) and minimal microprocessor-dependent code

IV. CHALLENGES

1) Security and Privacy: Security measures must be instituted in the development of 4G Wireless Networks which will facilitate the safest possible technique for data Transmission. Explicitly, "The 4G core delivers mobility, security, and QoS by means of reusing the existing methods while still working on a few mobility and handover concerns" [5]. Hence, for securing data, to be transmitted across the network, from hackers and further security contraventions it is obligatory for the organization to develop an efficient and effective series of tools which will support the utmost 4G security measures. As a result of the nature of the 4G wireless network, there is a more possibility of security intrusions, and hence, manifold levels of security, including increased necessities for validation, will be essential for protecting data and information transmitted across the network. One of the major objectives of 4G networks that exchange different sorts of data complicates the privacy and security concerns. Moreover, since new gadgets and services are being introduced for the first time in 4G wireless networks, the encryption and decryption schemes being used for 3G wireless networks are not suitable for 4G wireless networks. To prevail over these issues, two methods can be followed. The former method relies on modifying the current privacy and security methods so as to employ them to heterogeneous 4G wireless networks.

2) Quality of Service: Regarding the network quality, various telecommunication service providers assure the users for the enhanced connectivity, and the utmost possible data quality which is transmitted across the network, just as Ericsson's 4G Wireless Networks for TeliaSonera [5]. With the data rates of almost 10 times higher as compared to today's conventional mobile broadband networks and real-time performance, it allows users to be connected always, even "on the move". Consequently, it is essential for service providers to develop an efficient and effective method to the 4G Wireless Networks which will improve quality, bestows effectual security measures, and will make sure that all users are provided with widespread options for downloading music, video, and picture files without any delays. The major confront for 4G wireless networks is incorporating IP-based and non-IP-based gadgets. We know that gadgets which are non-IP address based are usually used for services such as VoIP. In contrast, gadgets which are IP address based are generally used for delivering data [5].

V. PRINCIPAL TECHNOLOGIES USED IN 4G

A) OFDM (Orthogonal Frequency Division Multiplexing):- OFDM increases bandwidth by splitting a data-bearing radio signal into smaller signal sets and modulating each onto a different subcarrier, transmitting them simultaneously at different frequencies. The subcarriers are spaced orthogonally and thus large numbers can be packed closely together with minimal interference. To maintain orthogonally among the tones, a cyclic prefix is added, the length of which is greater than the expected delay spread. With proper coding and interleaving across frequencies, multipath becomes an OFDM system advantage by yielding frequency diversity. OFDM can be implemented efficiently by using fast Fourier transforms (FFTs) at the transmitter and receiver.

B) MIMO (Multiple Input-Multiple Output):- MIMO is a spatial diversity technique that increases coverage or data capacity by either transmitting the same data on different antennas or different data on different antennas. A high-performance 4G broadband wireless mobile service requires multiple antennas be used at both the base station and subscriber ends. Multiple antenna technologies enable high capacities suited for internet and multimedia services and also dramatically increase range and reliability. Multiple antennas at the transmitter and receiver provide diversity in a fading environment. By employing multiple antennas, multiple spatial channels are created, making it unlikely that all channels fade simultaneously. With MIMO, the channel response becomes a matrix. Because each narrow band carrier can be equalized independently, the complexity of space-time equalizers is avoided.

VI. EVOLUTION OF MOBILE WIMAX TECHNOLOGY

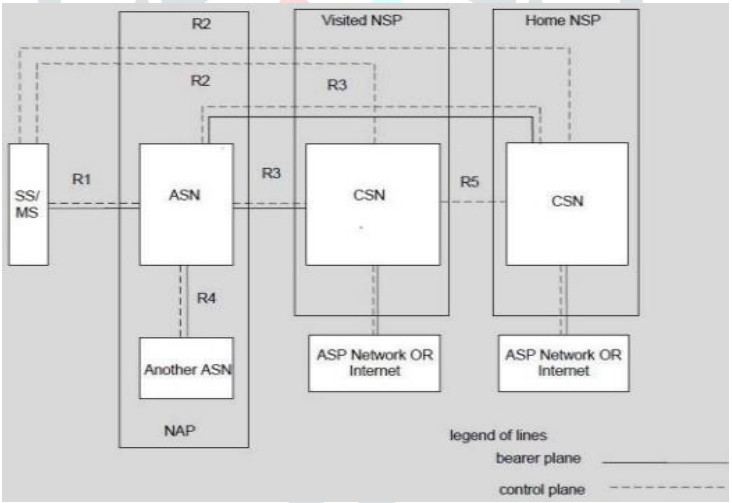
Mobile WiMAX has turned out to be a vital part of today's modern and digitized world. As a result, people are now showing more dependency on mobile computing. The demand for downloading and transporting the data on mobile devices moving with high speed has stirred up the development of new techniques so as to meet the various requirements of mobile computing. In the field of wireless networks our world has witnessed numerous revolutionary changes in the last two decades. Today wireless network has become an essential part of peoples' life in their day to day requirements and is becoming more popular by each passing day due to the necessity of mobility along with high speed broadband access. Presently, new and fast emerging technologies are being introduced in the field of wireless networks which allow high speed broadband wireless access. Mobile WiMAX, stands for Worldwide Interoperability for Microwave Access, is a sophisticated next generation mobile broadband wireless network based on IEEE 802.16e-2005[7] which supports 4G. Primarily it was developed for the solutions of problems faced by wired networks but later it became the part of 4G wireless network with the improvements from 802.16-2004, 802.16e-2005 to 802.16m. IEEE 802.16e -2005 is an improvement to IEEE 802.16 -2004[8] and the latter was the fixed data transmission technique for broadband connection to MAN. Wireless MAN-OFDMA specification assists in providing an enhanced air interface for operation in either unlicensed or licensed bands. Nowadays user wants to remain online every time and also want speedy transmission of data at low price without any data loss. Presently a large number of PDAs (Personal Digital Assistance) in the market are capable of supporting wireless data transmission flawlessly with mobility. In the upcoming future such type of requirement will raise immensely, therefore developers (for example WiMAX Forum) are looking for such type of requirements for making these gadgets more supportive in accordance with the user necessities. WiMAX (802.16e-2005) is the solution for such type of problems. WiMAX can support data rates up to 75 Mbps with a range of nearly about 30 miles.

VII. Architecture of WiMAX

The basic devices of WiMAX are of two types: WiMAX base-station and WiMAX receiver. The former is similar to a cellular tower, whereas, the latter could be a standalone tower or a Personal Computer Memory Card International Association (PCMCIA) card inserted into the laptop.

The WiMAX architecture developed by the WiMAX forum is unified network architecture to support fixed, nomadic and mobile operation. Fig. 1 represents the WiMAX Network Reference Model. The major elements or areas of WiMAX network architecture are:

A. Remote or Mobile Stations These are the user equipment's that may be mobile or fixed and may be located in the premises of the user.



B. Access Service Network (ASN): This is the area of the WiMAX network that forms the radio access network at the edge and it comprises one or more base stations and one or more ASN gateways.

C. Connectivity Service Network (CSN) This part of the WiMAX network provides the IP connectivity and all the IP core network functions.

D. Subscriber Station (SS) / Mobile Station (MS) the SS is also referred as the Customer Premises Equipment (CPE). These take a variety of forms and these may be termed either indoor CPE or outdoor CPE. The outdoor CPE has the advantage that it provides better performance as a result of the better position of the antenna, whereas the indoor CPE can be installed by the user. MS's are mostly used in the form of modem for a laptop.

E. Base Station (BS) The base-station forms an essential element of the WiMAX network. It is responsible for providing the air interface to the subscriber and mobile stations. It provides additional functionality in terms of micro-mobility management functions, such as handoff triggering and tunnel establishment, radio resource management, QoS policy enforcement, traffic classification, Dynamic Host Control Protocol (DHCP) proxy, key management, session management, and multicast group management.

F. ASN Gateway (ASN-GW) The ASN-GW in the WiMAX network architecture typically acts as a layer 2 traffic aggregation points within the overall ASN. The ASN-GW may also provide additional functions that include: intra-ASN location management and paging, radio resource management and admission control, caching of subscriber profiles and encryption keys. The ASN-GW may also include the Authentication, Authorization and Accounting (AAA) Server client functionality,

establishment and management of mobility tunnel with base stations, foreign agent functionality for mobile IP, QoS and policy enforcement, and routing to the selected CSN.

G. Home Agent (HA) The HA in the WiMAX network is located within the CSN. Mobile-IP forms a key element within WiMAX technology, the HA works in conjunction with a "Foreign Agent", such as the ASN Gateway, to provide an efficient end-to-end Mobile IP solution. The Home Agent serves as an anchor point for subscribers, providing secure roaming with QOS capabilities.

VIII: LONG TERM EVOLUTION

LTE Overview: LTE has improved the Universal Mobile Telecommunication Services (UMTS) in a series of points on account of the requirements of future generation cellular technology and rising mobile communication services necessities. Such improvements are generated owing to LTE background needs, motivations and objectives. The concise account concerning LTE technique and specifications is also being covered in the following subsections.

LTE Architecture:

The presently agreed LTE architecture employs a flat architecture, that can be demonstrated by the use of four functional elements as discussed below (see also Figure 2) [15]:

A. Evolved Radio Access Network (RAN): It primarily constitutes a single RAN node termed as eNodeB (eNB). The eNB hosts the physical layer (PHY), Medium Access Control (MAC), Radio Link Control (RLC), and Packet Data Control Protocol (PDCP) layers and interfaces with the User Equipment (UE). Its functions include admission control, radio resource management, scheduling and enforcement of negotiated UL QoS and compression/decompression of Downlink/Uplink user plane packet headers.

B. Serving Gateway (SGW): It works as the mobility anchor between LTE and other 3GPP technologies for the user plane during inter-eNB handovers. Simultaneously, it directs and forwards the user data packets. While Downlink data approaches UE the SGW functions in controlling the termination of the Downlink data path and imitates the user traffic during lawful and rational interception. In addition it also manages and stores UE information such as network internal routing information, parameters of the IP bearer service.

C. Mobility Management Entity (MME): It is the key control-node for the LTE access network which tracks and pages the idle mode UE, even during retransmission. MME chooses the SGW for a UE at first attach and at the time of intra-LTE handover which involves Core Network (CN) node relocation. During the authentication of the user, it interacts with the HSS (a master user database which supports IP Multimedia Subsystem including subscriber information) [16] through the specified interface.

D. Packet Data Network Gateway (PDN GW): It has two major tasks in terms of functionality. Foremost, the PDN GW supports the connectivity to the UE and also to the external packet data networks by the entry and exit of UE traffic. The other major role of the PDN GW is to act as a mobility anchor between 3GPP and non-3GPP technologies, for instance, WiMAX and 3GPP2 (CDMA 1X and EvDo).

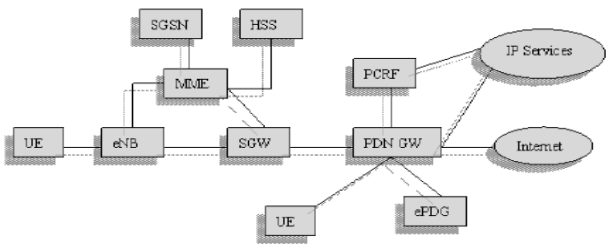


Figure 2: High Level Architecture for 3GPP LTE

IX: 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)
(iii) Illegal access and usage of security procedure keys to access network services (iv)
(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, and 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.

X. 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] G. J. Foschini andM. J. Gans, "On limits of wireless communications in a fading environment when using multiple antennas," Wireless Personal Commun.: Kluwer Academic Press, no. 6, pp. 311–335, 1998.
[8] A. Nosratinia, T.E. Hunter, A. Hedayat, "Cooperative communication in wireless networks," IEEE Communications Magazine, vol.42, no.10, pp. 74-80, Oct. 2004.
[9] G. Kramer, M.Gastpar, P.Gupta, "Cooperative Strategies and Capacity Theorems for Relay Networks," IEEE Transactions on Information Theory, vol.51, no.9, pp. 3037-3063, Sept. 2005.
[10] A. Host-Madsen, "Capacity bounds for Cooperative diversity," IEEE Transactions on Information Theory, vol.52, no.4, pp.1522-1544, April 2006.
[11] C. Santivanez, R. Ramanathan, C. Partridge, R. Krishnan, M. Condell, S.Polit, "Opportunistic Spectrum Access: Challenges, Architecture, Protocols," WiCon 2006, August, 2006.
[10] Y. Xing, R. Chandramouli, S. Mangold, S. Shankar, "Dynamic Spectrum Access in Open Spectrum Wireless Networks," IEEE Journal on Selected Areas in Communications, vol. 24, No. 3, pp 626-637, March 2006.
[11] I. Akyildiz, W. Lee, M. Vuran, S. Mohanty, "NeXt Generation/Dynamic Spectrum Access/Cognitive Radio Wireless Networks: A Survey," Elsevier Computer Networks, Vol 50, pp. 2127-2159, 2006.
[12] E. Buracchini , "The software radio concept," IEEE Communications Magazine, vol.38, no.9, pp.138-143, Sep 2000.
[13] H. Wally, W. Tuttlebee, "Software defined radio: enabling technologies", John Wiley and Sons, 2002.
[14] R. Bagheri, A.Mirzaei, M.E. Heidari, S. Chehrazi,Lee Minjae, M. Mikhemar, W.K. Tang, A.A. Abidi , "Software-defined radio receiver: dream to reality," IEEE Communications Magazine, vol.44, no.8, pp.111-118, Aug. 2006.
[15] J. Mitola, Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio, PhD Thesis, Royal Institute of Technology (KTH) 2000.