FOURTH GENERATION OF MOBILE COMMUNICATION NETWORK: EVOLUTION, PROSPECTS, OBJECTIVES, CHALLENGES AND SECURITY

Abdur Rahman*

Kapil Sharma*

ABSTRACT

Analyzing the attractive evolution of wireless communication, the much anticipated 4G standard promises wonders. This paper explores the trends in the evolution of wireless communication and its security. It outlines the requirements that are to be met by the 4G standard and also attempts to analyze the technical challenges that demand solutions during the course of the development and implementation of the next generation of wireless communication. Further, It presents the possible application areas of the 4G standard and the research areas that have been identified for development and stabilization of the 4G standard. The 4G work started in 2005 and 4G wireless network full complete development approx in mid 2015 in all country Research and industry communities are racing against time to find solutions for open issues in 4G networks.

Keywords: *Evolution of Mobile Communication, Requirements of 4G networks, Technical Challenges, Potential Application Areas of 4G network, Standardization Activities, Security requirements of 4G networks, Security Architecture, Security issues of 4G network, Security Analysis.*

*School of Information and Communication Technology, Gautam Buddha University, Greater Noida

1. EVOLUTION OF MOBILE COMMUNICATION SYSTEMS

Evolution of Wireless Communication has been rapid. Demands for further development have surfaced even faster. These demands have instigated innovations. From the age of pre-cellular mobile telephone technology, referred to as 0G in some literatures, till date wireless communication has been through remarkable changes.

1G technology replaced 0G technology, 1G stands for "first generation", refers to the first generation of wireless telecommunication technology, more popularly known as cell phones. A set of wireless standards developed in the 1980's[1]. The first generation of wireless mobile communications was based on analog signalling. Analog systems, implemented in North America, were known as Analog Mobile Phone Systems (AMPS), while systems implemented in Europe and the rest of the world were typically identified as a variation of Total Access Communication Systems (TACS). Analog systems were primarily based on circuit-switched technology and designed for voice, not data[2]. This Phone System AMPS was a frequency modulated analog mobile radio system using frequency Division Multiple Access (FDMA) with 30kHz channels occupying the 824MHz-894MHz frequency band and a first commercial cellular system deployed until the early 1990’s [3].

Second Generation rapid growth in the number of subscribers and the proliferation of many incompatible first generation systems were the main reason behind the evolution towards second generation cellular systems. Second generation systems take the advantage of compression and coding techniques associated with digital technology. All the second generation systems employ digital modulation schemes. Multiple access techniques like Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA) are used along with FDMA in the second generation systems.

Second generation cellular systems include:

- United States Digital Cellular (USDC) standards IS-54 and IS-136
- Global System for Mobile communications (GSM)
- Pacific Digital Cellular (PDC)
- Cdma One[4].

2G based on the two techniques, there were three primary 2G mobile communication systems. They are TDMA (IS-136), CDMA (IS-95), and GSM [5]. TDMA (IS-136), as a completely digital system, was deployed in North America in 1993, but operated in the AMPS frequency band of 824MHz-894MHz. CDMA (IS-95) systems using Direct Sequence Spread Spectrum (DSSS) are working on the 1850-1990 MHz frequency band to support

CDMA carriers. This spectrum is commonly called Personal Communications Services (PCS). GSM is the most widely used 2G standard, accounting for about 66 percent of the world market in the year 2004 [6]. Standards were developed to provide both data service, and increase the data rate in GSM networks. General Packet Radio Service (GPRS) was a packet overlay network designed to provide data services in a GSM network. GPRS utilized the same frame structure as GSM, and supported a maximum data rate of 21.4kbps [7].

2.5G GPRS (General Packet Radio Service) Until the late nineteen-nineties wireless mobile networks focused primarily on voice service, evolving from the well known “bag telephone” in the late eighties to the newer, clearer digital networks, such as GSM. With the advent of smaller, more powerful devices, user sophistication has grown and with it the demand for faster wireless data services has also grown. In an attempt to address this, the European Telecommunications Standards Institute (ETSI) developed a new wireless data network, designed to integrate with existing digital networks, known as General Packet Radio Service or GPRS. GPRS offers speeds from 9 to 115 Kbps and support for multiple bandwidths, make it an ideal solution for carriers on the path to the 3G. In fact, GPRS can be added to a network incrementally, allowing the total capacity to be increased as needed. This approach has two advantages, it minimizes the risk on the investment required to deploy a GPRS network, and allows the users to drive the deployment[8].

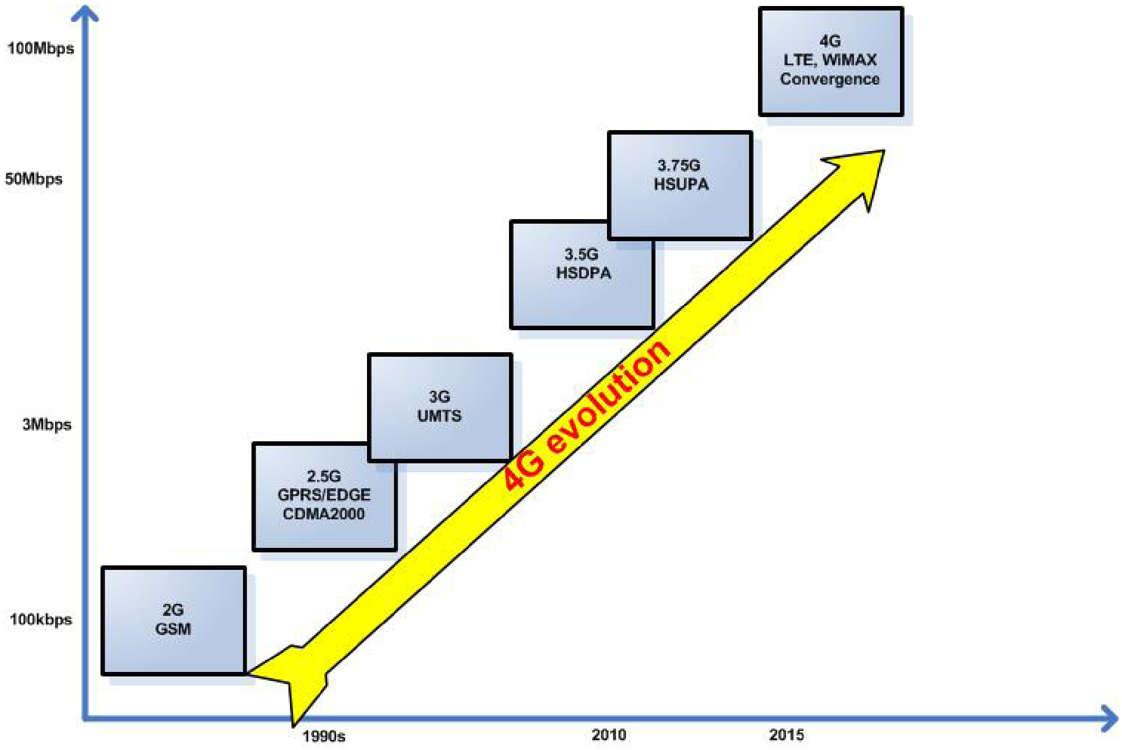

Fig. 1. Evolution of 4G technology

The phase after GPRS is called Enhanced Data Rates for GSM Evolution (EDGE) 2.75, generally considered a 3G technology, introduces new methods at the physical layer, including a new form of modulation (8 PSK) and different ways of encoding data to protect against errors. But the higher layer protocols stay the same. Thus EDGE can deliver maximum data rates up to 500 Kbps using the same GPRS infrastructure (practical throughputs may be only half the maximum rate). EDGE has been designed to address some of the limitations of GPRS. For example, GPRS impacts a network's existing cell capacity because voice and GPRS calls both use the same network resources.

Third generation program started in 1985 with the Project name Future Public Land Mobile Telephone System (FPLMTS). 3G cellular systems are being designed to support wideband services like high speed Internet access, video and high quality image transmission with the same quality as the fixed networks.

The primary requirements of the next generation cellular systems are [9]:

- Voice quality comparable to Public Switched Telephone Network (PSTN).
- Support of both packet-switched and circuit-switched data services.
- More efficient usage of the available radio spectrum
- Support of high data rate. The following table shows the data rate requirement of the 3G systems

Table 1. 3G Data Rate Requirements

Mobility Needs	Minimum Data Rate
Vehicular	144 kbps
Outdoor to indoor and pedestrian	384 kbps
Indoor Office	2 Mbps

- Support of a wide variety of mobile equipment
- Backward Compatibility with pre-existing networks and flexible introduction of new services
- An adaptive radio interface suited to the highly asymmetric nature of most Internet communications: a much greater bandwidth for the downlink than the uplink.

3G technologies make use of TDMA and CDMA.3G technologies make use of value added services like mobile television, GPS (global positioning system) and video conferencing. Additional features also include HSPA data transmission capabilities able to deliver speeds up to 14.4Mbit/s on the downlink and 5.8Mbit/s on the uplink. Spectral efficiency or spectrum efficiency refers to the amount of information that can be transmitted over a given bandwidth in a specific digital communication system. ... High-Speed Packet Access (HSPA) is a collection of mobile telephony protocols that extend and improve the performance of existing UMTS protocols. After ten years of development, IMT-2000 (International Mobile Telecommunications-2000) has accepted a new 3G standard from China, i.e TD-SCDMA. Thus, there are new three 3G cellular network standards. They are CDMA2000 from America, WCDMA from Europe and TD-SCDMA from China [10]. 3G technology is much flexible, because it is able to support the 5 major radio technologies. These radio technologies operate under CDMA, TDMA and FDMA.CDMA holds for IMT-DS (direct spread), IMT-MC (multi carrier). TDMA accounts for IMTTC (time code), IMT-SC (single carrier). FDMA has only one radio interface known as IMT-FC or frequency code. There are many 3G technologies as GSM EDGE, UMTS, W-CDMA, DECT, WiMax and CDMA 2000.Enhanced data rates for GSM evolution or EDGE is termed to as a backward digital technology, because it can operate with older devices.

3.5G High Speed Downlink Packet Access (HSDPA) is a mobile telephony protocol, also called the 3.5G. HSDPA supports the high bit rate data services and will increase network capacity, while minimizing operators’ investment. It provides a smooth evolutionary path for Universal Mobile telecommunications System (UMTS) networks to higher data rates and higher capacities. HSDPA are fast link adaptation, fast scheduling and currently being developed within the 3GPP framework[11].

3.75G High-Speed Uplink Packet Access (HSUPA) is a 3GPP release 6 feature for WCDMA. Objective is to achieve uplink data rates of up to 5.76 Mbps and increase throughput and capacity. HSUPA is the next evolution step for UMTS networks. The technology which is also known as FDD Enhanced Uplink (EUL) has been introduced in the release 6 of 3GPP standards. Objective of HSUPA is to enhance uplink packet data transmission by achieving data rates of up to 5.76 Mbps. Furthermore, HSUPA will increase uplink capacity and reduce latency. A combination of HSDPA and HSUPA is especially beneficial, since it will allow optimized packet data transfer in downlink and uplink. Services that benefit from HSUPA are multimedia applications requiring excellent uplink performance, e.g. gaming, video streaming, file upload[12].

The 4G work started in 2005. Initially the most likely 4G candidate technologies were announced to be IEEEs 802.16e standard (Mobile WiMAX) and 3GPPs LTE. 4G refers to the fourth generation of cellular wireless standards. It is a successor to 3G and 2G families of standards[13,14,15,16]. The 4G mobile system is an all IP-based network system. The features of 4G may be summarized with one word—integration[17]. The 4G systems are about seamlessly integrating different technologies and networks to satisfy increasing user demands [18,19]. 4G technologies shall combine different current existing and future wireless network technologies (e.g. IPv6, OFDM, MC-CDMA, LAS-CDMA and Network-LMDS) to ensure freedom of movement and seamless roam from one technology to another.

IPv6 is basic protocol for address issue in 4G networks. OFDM stands for orthogonal frequency Division Multiplexing, which transmitting large amounts of digital data over a radio wave. OFDM works by splitting the radio signal into multiple smaller sub signals that are then transmitted simultaneously at different frequencies to the receiver. LAS-CDMA stands for Large Area Synchronized Code Division Multiple Access, which enables high-speed data and increases voice capacity. It is designed for global area. MS-CDMA stands for Multi-Carrier Code Division Multiple Access, which is designed for running on wide area, called macro cell. The Network-LMDS, Local Multipoint Distribution System, is the broadband wireless technology used to carry voice, data, internet and video services in 25GHz and higher spectrum. It is designed for micro cell. Ericsson and the University of California are jointly researching CDMA wireless access technology, advanced antenna systems, next-generation mobile Internet, quality of service, power amplifier technology, and wireless access networks. Other 4G applications include high-performance streaming of multimedia content based on agent technology and scalable media coding methods. 4G will solve problems like limited bandwidth in 3G when people are moving and uncertainty about the availability of bandwidth for streaming to all users at all times.

One of the key requirements is to realise a wireless 4G IP-based access system. The ultimate objective is to create a protocol suite and radio communication schemes to achieve broadband mobile communication in 4G wireless systems. A new protocol suite for 4G wireless systems supported by Department of Defence (DoD) contains:

- Transport-layer protocols
- Error-control protocols
- Medium-access protocol
- Mobility management
- Simulation test bed
- Physical test bed
- Protocol suite in the mobile terminal
- Protocol suite in the base station[20].

2. REQUIREMENTS FOR 4G SYSTEM

A) Broadband Wireless Access

The traffic carried by mobile communication systems until today was mainly for voice communications. The Second-Generation (2G) system, the Personal Digital Cellular (PDC) system, introduced the i-mode services, which enabled the Internet access, electronic commerce and e-mail from mobile terminals, and mainly used for the text-based data communications. The IMT-2000 system offers high bit rate transmission service from 64 kbit/s to 384 kbit/s, and it is expected that the proportion of the amount of data traffic to the voice traffic would continue to increase. Moreover, the rising popularity of broadband services such as Asymmetric Digital Subscriber Line (ADSL) and optical fiber access systems and office or home LANs is likely to lead to a demand for comparable services in the mobile communication environment[21].

B) High network capacity:

Through the use of efficient multiple access schemes (e.g. Orthogonal FDMA OFDMA), Single Carrier FDMA, Interleaved FDMA and Multi-carrier code division multiple access (MC-CDMA)) and advanced antenna systems, often referred to as smart antennas or intelligent antennas, 4G standards require to provide higher network capacity[22].

C) Low Cost

To make broadband services available to the user to exchange various kinds of information, it is necessary to lower charges dramatically in order to keep the cost at or below the cost of existing service. The IMT-2000 system aimed at lower bit cost and economical charge rates, however for the 4G system, a broadband channel and an even lower bit cost are both required[21].

D) Seamless connectivity and global roaming across multiple heterogeneous networks:

Issue of heterogeneity must be addressed in 4G standards. To support the idea of ubiquity, 4G standards must provide means of seamless connectivity and handoff across these heterogeneous (i.e. networks of different scales and functionalities) networks. Vertical and Horizontal handovers are critical for 4G. Moreover a smooth transitioning from the existing wireless standards to the 4G standards is equally important to ensure popularity and commercial viability[22].

E) Wide Area Coverage

One feature of mobile communications is that it is available for use anytime and anywhere. That advantage is important for future mobile communication as well. In particular, it is important to maintain the service area in which the terminals of the new system can be used during the transition from the existing system to a new system. It can be assumed that terminals that have relatively large display screens, such as Personal Digital Assistants (PDAs) or personal computers are used indoors rather than outdoors. Accordingly, better coverage of indoor service areas is needed[21].

3. TECHNICAL CHALLENGES

In order to meet the above mentioned requirements communication engineers need to overcome the following technical challenges and barriers.

A) Security and Privacy

In the development of 4G Networks, security measures must be established that enable data transmission to be as safe as possible. Specifically, “The 4G core addresses mobility, security, and QoS through reuse of existing mechanisms while still trying to work on some mobility and handover issues”. Therefore, it is necessary for the organization to develop an effective series of tools that support maximum 4G security measures as a means of protecting data that is transmitted across the network from hackers and other security violations. Because of the nature of the 4G network, there is an increased likelihood of security attacks, and therefore, multiple levels of security, including increased requirements for authentication, will be necessary to protect data and information that is transmitted across the network [24].

One of the main goals of G4 networks is to blanket very wide geographic area with seamless service. Obviously, smaller local area networks will run different operating systems. The heterogeneity of these wireless networks exchanging different types of data complicates the security and privacy issues. Furthermore, the encryption and decryption methods being used for 3G networks are not appropriate for 4G networks as new devices and services are introduced for the first time in 4G networks. To overcome these security and privacy issues, two approaches can be followed. The first is to modify the existing security and privacy methods so that they will be applicable to heterogeneous 4G networks. Another approach is to develop new dynamic reconfigurable, adaptive, and lightweight mechanisms whenever the currently utilized methods cannot be adapted to 4G networks [25].

B) Technologies for Cost Reduction

The use of higher frequency band to achieve higher transmission rate with conventional system configuration technology generally reduces the radius of the cell that one base station can cover. To retain the original coverage area, more base stations are required and network cost is increased. To avert that problem, it is necessary to expand cell radii by means of higher performance radio transmission and circuit technology, such as improved modulation/demodulation techniques that can cope with low S/N, the use of adaptive array antennas, and low noise receivers[21].

C) Quality of Services

What QoS does 4G provide to us they are as follows:-

(1) Traffic generated by the different services will not only increase traffic loads on the networks, but will also require different quality of service (QoS) requirements (e.g., cell loss rate, delay, and jitter) for different streams (e.g., video, voice, data).

(2) Providing QoS guarantees in 4G networks is a non-trivial issue where both QoS signaling across different networks and service differentiation between mobile flows will have to be addressed.

(3) One of the most difficult problems that are to be solved, when it comes to IP mobility, is how to insure the constant QoS level during the handover.

(4) Depending on whether the new access router is in the same or some other sub network, we recognize the horizontal and vertical handover.

(5) However, the mobile terminal cannot receive IP packets while the process of handover is finished. This time is called the handover latency.

(6) Handover latency has a great influence on the flow of multimedia applications in real-time.

D) Complex Architecture

1) Multimode End-User Terminals

To reduce operating costs, devices that operate on 4G networks should have the capability to operate in different networks. This will not only reduce the operating cost but will also simplify design problems and will reduce power consumption. However, accessing different mobile and wireless networks simultaneously is one of the major issues 4G networks have been addressing[23].

2) System Discovery and Selection

Due to the heterogeneity of 4G networks, wireless devices have to process signals sent from different systems, discover available services, and connect to appropriate service providers. Various service providers have their own protocols which can be incompatible with each other as well as with the user’s device. This issue may complicate the process of selecting the most appropriate technology based on the time, place and service provided, and thus, may affect the Quality of service provided to the end user. One solution to resolve this issue is called “System initiated discoveries”. This mechanism allows automatic download of software modules based on the wireless system the user is connected to [26].

3) Service and Billing

Managing user accounts and billing them has become much more complicated with 4G networks. This is mainly due to heterogeneity of 4G networks and the frequent interaction of service providers. The research community addressed this concern and proposed several frameworks to handle the customers’ billing and user account information[27,28].

4. POTENTIAL APPLICATION AREAS OF 4G

Some of the potential applications of 4G are [29]:

A) Virtual Presence: The ubiquitous theme of 4G system together with the idea of enhanced-reality multi-media communication gives mobile users a "virtual presence". For example, always-on connections that keep people involved in business activities regardless of whether they are on-site or off

B) Virtual Navigation: Information about people and locations stored in the central databases can be accessed rapidly and reliably through the use of 4G standards. The destination terminal can thus enjoy virtual navigation. This can be deployed in countless cases ranging from navy applications to calamities or crime control to fun games.

C) Tele-medicine: 4G will support remote health monitoring of patients. With the proper application of technology in such cases the medical access can be extended to places where medical personnel cannot avail themselves readily.

D) Tele-Geo processing Applications: The combination of geographical information systems (GIS), global positioning systems (GPS), and high capacity wireless mobile systems will enable a new type of application referred to as tele-geo processing. Queries dependent on location information of several users, in addition to temporal aspects have many applications.

E) Crisis-Management Applications: Natural disasters can affect the entire communications infrastructure is in disarray. Restoring communications quickly is essential. With wideband wireless mobile communications Internet and video services, could be set up in hours instead of days or even weeks required for restoration of wire line communications.

5. STANDARDIZATION ACTIVITIES

The two groups within the International Telecommunication Union (ITU) are specifically engaged to define the next generation of wireless communication. Thesetwo groups are:

- Working Party 8F (WP8F) in section ITU-R
- Special Study Group (SSG) “IMT 2000 and Beyond” in section ITU-T

WP8F is focused on the overall radio-system aspects of 4G, such as radio interfaces, radio-access networks. In April, 2007, the ITU convened a global congress to set a course for the 4G standards development process. The\ World Radio communication Conference (WRC) in October/ November 2007 at Switzerland decided on the spectrum assignment for 4G. This has cleared the way forward for defining technologies and standards. The road map of the ITU-R (International Telecommunication Union Radio communication Sector) targets the availability of 4G standard proposals for the year 2012. As soon as frequency bands for 4G are defined, 4G standardization activities are expected to start[30].

6. SECURITY REQUIREMENTS OF 4G NETWORKS

According to the four kinds of security threats on 4G wireless networks, which are associated with attack on the ME/USIM, radio interface, radio network operator and IP bone networks separately, we list corresponding security requirements briefly as the follows[31].

(A) Security requirements on ME/USIM:

- It shall protect the integrity of the hardware, software and OS in mobile platform.
- It shall control access to data in ME/USIM.
- It shall to protect the confidentiality and integrity of data stored in the ME/USIM or transported on the interface between ME and USIM.
- It shall retain user’s identity as privacy to ME.

(B) Security requirements on radio interface and network operator:

- Entity authentication: mutual authentication between user and network shall be implemented to ensure secure service access and provision.
- Ensure confidentiality of data including user traffic and signaling data on wired or wireless interface.
- Lawful interception: It shall be possible for law enforcement agencies to monitor and intercept every call in accordance with national laws.

(C) Security visibility, configurability and scalability:

- The security features of the visited network should be transparent to user.
- The user can negotiate acceptable security lever with the visited network when user roams outside HE (home environment).
- The security mechanism shall be scalable to support increase of user and/or network elements.

7. THE SECURITY ARCHITECTURE

A) Objectives

Traditionally, the network security has focused on securing network edges to prevent external threats from accessing network resources. However, this approach is not adequate because the attackers seek to discover security vulnerabilities in networking protocols, operating systems or applications, and exploit these vulnerabilities to propagate malware that may evade security measures at the edges. Hence, we need a comprehensive, network-wide security architecture integrated into both the network core and the end user

devices. The key objectives in designing the security architecture can be summarized as:

- *availability* that enforces networks and services not to be disrupted or interrupted by, for example, malicious attacks;
- *interoperability* that ensures the security solutions can avoid interoperability problems, e.g., by using generic solutions applicable to most of the NGN applications and service scenarios;
- *usability* that makes it easy for the end-users to use the security-enabled services;
- *cost-effectiveness* that minimizes the additional cost of security and makes it lower than the cost of risks[32].

B) Threat Model

Possible threats to 4G include: IP address spoofing, user ID theft, Theft of Service (ToS), DoS, and intrusion attacks. Among them, network operators are concerned about ToS and DoS attacks because they will harm their revenue, reputation and service availability. The security threats are further categorized, according to X.805 [33], as:

destruction of information and/or other resources,

- corruption or modification of information,
- theft, removal or loss of information and/or other resources,
- disclosure of information, and
- interruption of services.

Besides this general categorization, protocol-specific attacks must be identified. For example, SIP-targeted attacks [?] include: (i) malformed message attacks, (ii) buffer overflow attacks, (iii) Denial-of-Service (DoS) attacks, (iv) RTP session hijacking, (v) injection of unauthentic RTP, (vi) reuse of compromised SIP credentials, and (vii) bogus SIP network elements.

It is almost impossible to make a 100% secure system because new threats and vulnerabilities will continue to take place. Also, there exist different stakeholders including at least network operators, service providers and users, having their own, sometimes mutually contradictory, interest, leading to different security requirements. Hence, the 4G security architecture must be flexible enough to adapt itself to future threats and vulnerabilities as well as varying security requirements[35].

C) IMS Security Architecture

The IP Multimedia Subsystem (IMS) is essentially an overlay on top of the network infrastructure such as 3GPP. The goal of IMS security is to protect all IMS sessions between the end-users and IMS servers, by offering its own authentication and authorization mechanisms as well as communication flow protection [34]. The two parts of IMS security are described below.

- **The first-hop security** secures the first hop from the end-user to the Proxy Call Session Control Function (P-CSCF). It uses an individual security context for each user, based on IMS Subscriber Identity Module (ISIM) on the Universal Integrated Circuit Card (UICC) placed at the end-user device.
- **The network domain security** (NDS) protects the rest of hops between CSCFs inside the IMS core. It is further divided into inter-domain and intra-domain interfaces, which represent the interfaces between two different security domains and between components within the same security domain, respectively.

As the first-hop (or the first-mile) provides users with a means to access the IMS infrastructure, it should apply very strong security ranging from authentication of end-user that prevents user identity theft to integrity protection of the end-user’s signaling that defeat ToS and other malicious attacks exploiting the signaling. By contrast, the network domain security enables the network operators to build their own IMS network and to have security mechanisms interoperate with other operators[35].

D) NGN Security Architecture

The NGN security mostly inherits the IMS security because IMS is inherently independent of the access technology. In other words, it can be viewed as the IMS security over fixed/mobile broadband access [34].

The entire NGN is divided into security domains, each maintained under the sole responsibility of network operator. Similarly to IMS, the NGN security consists of:

- **access view security** that secures the first-hop for the end-user device to access the network;
- **NGN core view security** that covers security within a intra-operator domain; and

- **interconnecting view security** that secures the inter operator domain.

It is challenging to achieve an adequate level of security due to the heterogeneous nature of NGNs. For example, network authentication between the end-user device and the Network Access Sub-System (NASS) strongly depends on the access technology. The access view security uses IPsec transport mode and Authentication and Key Agreement (AKA) on top of the ISIM application on UICC in the end-user device A unique requirement of NGN is its support for more business roles ranging from regional network operators to service providers. Hence, many of the external connectivity points will likely be inter-operator interfaces, which may become potential sources of vulnerabilities. To protect these interfaces, NGN specifies Security Gateways (SEGs) that enforce security policy between domains[35].

8. SECURITY ISSUES-4G WIRELESS

A) Physical Layer Issues

Both WiMAX and LTE are subject to two key vulnerabilities at the physical layer - Interference and Scrambling attacks [36]. 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 [37]. 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.

Interference attacks can be easily carried out as the equipment and knowledge to carry out such attacks are widely available. Our analysis indicates that interference is easy to detect using radio spectrum monitoring equipments. Using radio-direction-finding tools, the interfering source can be traced. In addition, increasing the power of the source signal and using spreading techniques can increase its resilience against interference. While the possibility of interference is significant, since it is easy to detect and address, we believe its impact on the WiMAX/LTE network and users will be limited[42].

B) WiMAX – MAC-Layer Security Issues

The IEEE 802.16 radio interface standard describes several steps in order for a MS 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. Steps 6 and 7 involve secure traffic exchange based on the device authentication standards of WiMAX.

There are various sources of potential vulnerabilities in WiMAX 802.16e [38,39,40,41]. Some of these sources include: (i) The fact that management MAC messages are never encrypted providing adversaries 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 vulnerabilities for WiMAX security[42].

C) LTE – MAC Layer Security Issues

One approach to categorizing LTE security issues is to group them as follows [43]: (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 a UE from normal services (v) wilful tampering of the eNB system broadcast information (vi) eavesdropping and illegal modification of IP packet contents (vii) Denial of Service attacks launched on the UE or eNB (viii) data integrity attacks (signaling or user data) using replay.

D) Security Issues at the Higher Layers

It is expected that a range of security risks will emerge in 4G wireless due to a number of factors including: (i) departure from proprietary operating systems for hand held devices to open and standardized operating systems and (ii) open nature of the network architecture and protocols (IP-based). With this move to open protocols and standards, 4G wireless networks are now susceptible to computer attack techniques present on the Internet. Such networks will be increasingly vulnerable to a range of security attacks including for example Malware, Trojans and Viruses [44].

9. SECURITY ANALYSIS

A) Objectives

The first step in analyzing cellular wireless security is to identify the security objectives. These are the goals that the security policy and corresponding technology should achieve. Howard, Walker, and Wright, of the British company Vodafone, created objectives for 3G wireless that are applicable to 4G as well:

- To ensure that information generated by or relating to a user is adequately protected against misuse or misappropriation.
- To ensure that the resources and services provided to users are adequately protected against misuse or misappropriation.
- To ensure that the security features are compatible with world-wide availability...
- To ensure that the security features are adequately standardized to ensure world-wide interoperability and roaming between different providers.
- To ensure that the implementation of security features and mechanisms can be extended and enhanced as required by new threats and services.
- To ensure that security features enable new ‘e-commerce’ services and other advanced applications(Howard, Walker, and Wright 2001, 22)

B) Threats

Because instances of 4G wireless systems currently only exist in a few laboratories, it is difficult to know exactly what security threats may be present in the future. However, one can still extrapolate based on past experience in wired network technology and wireless transmission. For instance, as mobile handheld devices become more complex, new layers of technological abstraction will be added. Thus, while lower layers may be fairly secure, software at a higher layer may introduce vulnerabilities, or vice-versa. Future cellular wireless devices will be known for their software applications, which will provide innovative new features to the user. Unfortunately, these applications will likely introduce new security holes, leading to more attacks on the application level (Howard, Walker, and Wright 2001, 22). Just as attacks over the Internet may currently take advantage of flaws in applications like Internet Explorer, so too may attacks in the future take advantage of popular applications on cellular phones. In addition, the aforementioned radio jammers may be adapted to use IP technology to masquerade as legitimate network devices[45].

10. CONCLUSION

Throughout the course of evolution of the wireless communication up to the fourth generation, and we discuss the requirement of 4G system, Technical Challenges, Potential Application Areas of 4G, Standardization Activities and main part of this paper Security requirements of 4G networks, The Security Architecture, Security Issues of 4G wireless, Security Analysis.

REFERENCES

[1] H.H. Chen, M. Guizani, W. Mohr, "Evolution toward 4G wireless networking", IEEE Network, 2005. Volume: 21 Issue: 1 pp. 4-5.

[2] T.D. Systems, "Third Generation (3G) Wireless", White Paper Inc. March 2000 Inc.

[3] C. Yiping, Y. Yuhang; "A new 4G architecture providing multimode terminals always best connected services", IEEE Wireless Communications, Volume: 14 Issue: 2 pp. 36-41.

[4]F. Alam, "Simulation of Third Generation CDMA Systems", MSc thesis, Dept of Electrical and Eng, Polytechnic Institute & State University, 1999. Virginia.

[5] S. Frattasi, A. Gimmler, "Potentials and limits of cooperation in wireless communications: Toward 4G wireless", IEEE Technology and Society Magazine, 2005. Volume: 27 Issue: 1 pp. 8-12.

[6] 3GPP. Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking (Release 6). 3GPP, TR 22.934 V6.1.0. http://www.3gpp.org/ftp/Specs/2002-12/Rel- 6/22_series/22934-610.zip.

[7] R, JP, "Mapping the wireless technology migration path: The evolution to 4G systems", Enriching Communications, Volume: 2 Issue: 1 pp. 73-79.

[8] M.R. Bhalla, A.V. Bhalla, "Generation of Mobile Wireless Technalogy: A Survey", IEEE International Journal of Computer Application, August 2010. vol. 5. No. 4. pp.26-32.

[9] M.W. Oliphant, " The Mobile Phone Meets the Internet," IEEE Spectrum, August 1999. pp. 20-28.

[10] X. Li, A. Gani, L. Yang, O. Zakaria, B. Jumaat, "Mix-Bandwidth Data Path Design for 5G Real Wireless World". The Proceeding of WSEAS 13th International Conferences on Multimedia and Communication, Crete Island,Greece, 21-23,July 2008. pp.216- 221.

[11] Application Note 1MA82; HSDPA Test and Measurement Requirements, Rohde & Schwarz.

[12] Rohde & Schwarz "High-Speed Uplink Packet Acccess" White Paper Application Note 1MA94.

[13] H. Chaouchi, G. Pujolle, I. Armuelles, M. Siebert, F. Bader, I. Ganchev, M. O’Droma, N. Houssos. “Policy Based Networking in the Integration Effort of 4G Networks and Services”. IEEE VTC04 Spring, Milan, May 2004.

[14] M. O'Droma, I. Ganchev, G. Morabito, R. Narcisi, N. Passas, S. Paskalis et al. “Always Best Connected Enabled 4G Wireless World”. ISBN 972-98368-7. June 2003. Pp.710-716.

[15] B. G. Evans and K. Baughan, "Visions of 4G," Electronics and Communication Engineering Journal, Dec. 2002.

[16] Frederic Paint, Paal Engelstad, Erik Vanem, Thomas Haslestad, Anne Mari Nordvik, Kjell Myksvoll, Stein Svaet, “Mobility aspects in 4G Networks- White Paper”.

[17] R. Salleh, X. Li, L. Yang, Z. Li, “Radio Frequency Convergence Protocol for 4G Networks”, Proceedings of the 8th WSEAS International Conference on Multimedia System and Signal Processing (MUSP ’08). April 6-8, 2008. Vol. 586, pp. 287-293.

[18] I. Ganchev, M. O’Droma, H. Chaouchi, I. Armuellus, M. Siebert, N. Houssos “Requirements for an Integrated System and Service 4G Architecture” IEEE 2004.

[19] J. P. Singh, T. Alpcan, X. Zhu, “Towards Heterogeneous Network Convergence: Policies and Middleware Architecture for Efficient Flow Assignment, Rate Allocation and Rate Control for Multimedia Applications”, MNCNA ’07, Port Beach- CA, USA, November 26, 2007.

[20] www.electronicsforu.com/EFYLinux/efyhome/.../Mobile-tech.pdf

[21] T. Miki, T. Ohya, H. Yoshino, N. Umeda, “The Overview of the 4th Generation Mobile Communication System”, IEEE 2005. Pp. 1551-1555.

[22] S.K. Subedi, “Fourth Generation of Mobile Communication Systems: Evolution, Objectives, Prospects and Challenges”, IEEE International Conference on Internet, 2009. pp. 1-6.

[23] K.P. Makhecha, K.P. Wandra, “4G Wireless Networks: Opportunities and Challenges”, IEEE INDICON 2009. Pp. 1-4

[24] E. Buracchini, “The Software Radio Concept,” IEEE Commun. Mag., 2000 vol. 38, no. 9, pp. 138–43.

[25] N. Montavont and T. Noel, “Handover Management for Mobile Nodes in IPv6 Networks,” IEEE Commun. Mag., Aug. 2002, vol. 40, no. 8, pp. 38–43.

[26] A. Lyle, Clear, first 4G network launched, 2009.

[27] F. Ghys and A. Vaaraniemi, “Component-based Charging in a Next generation Multimedia Network,” IEEE Commun. Mag., Jan. 2003, vol. 41, no. 1, pp. 99–102.

[28] S. Higgenbotham, Countdown to 4G: who’s doing what, when, 2008.

[29] Govil J., Govil J., 4G Mobile Communication Systems: Turns, Trends and Transition, IEEE Computer Society, 2007.

[30] eMobility Technology Platform Whitepaper, Beyond3G / 4G Radio Access Technologies (RATs) and Standards Roadmaps, 2007.

[31] Y. Zheng, D. He, W. Yu, X. Tang, "Trusted Computing-Based Security Architecture For 4G Mobile Networks", IEEE Conference on Parallel and Distributed Computing, Applications and Technologies, 2005, pp. 251-255 .

[32] Y. Park, T. Park, "A Survey of Security Threats on 4G Networks", IEEE Workshop on Security and Privacy in 4G Networks, Nov. 2007, pp. 1-6.

[33] ITU-T, "X.805: Security architecture for systems providing end-to-end communications", 2003.

[34] A. Bultinck, D. Hoefkens and M. Mampaey, "Security from 3GPP IMS to TISPAN NGN", Alcatel Telecommunications Review, 4th Quarter 2005.

[35] Y. Park, T. Park, "A Survey of Security Threats on 4G Networks", IEEE Workshop on Security and Privacy in 4G Networks, Nov. 2007, pp. 1-6.

[36] M. Barbeau, "Wimax/802.16 threat analysis", Proceedings of the 1st ACM international conference on Quality of Service & security in wireless and mobile networks. New York, 2005.

[37] M. Husso, "Performance Analysis of a WimAX System under Jamming", MSc thesis, Dept of Electrical and Communication Eng, Helsinki University of Technology, Finland, Dec. 2006.

[38] M. Barbeau, "Wimax/802.16 threat analysis", Proceedings of the 1st ACM international conference on Quality of Service & security in wireless and mobile networks. New York, 2005.

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

[40] Y. Park and T. Park, "A survey of Security Threats on 4G Networks", IEEE Globecom Workshop on Security and Privacy in 4G Networks, Nov. 2007, Washington, DC.

[41] P. Rengaraju et al, "Analysis on Mobile WiMAX Security", IEEE TICSTH Conf - Symposium on Information Assurance, Sept. 2009.

[42] N. Seddigh, B. Nandy, R. Makkar, J.F. Beaumont, "Security Advances and Challenges in 4g wireless networks", IEEE Eighth Annual International Conference on Privacy Security and Trust (PST), 17-19 Aug. 2010, pp. 62-71.

[43] C.B. Sankaran, “Network Access Security in Next Generation 3GPP Systems: A Tutorial”, IEEE Communications Magazine, Feb. 2009.

[44] J.F. Beaumont, G. Doucet, “Threats and Vulnerabilities of Next Generation Satellite Personal Communications Systems: A Defence Perspective”, IEEE Globecom Workshop on Security, and Privacy in 4G Networks, Nov. 2007, Washington.

[45] J. Ahmad, B. Garrison, J. Gruen, C. Kelly, and Hunter Pankey, “4G Wireless Systems”, Feb. 2003.