International Journal of Computer Architecture and Mobility

(ISSN 2319-9229) Volume 1-Issue 9, July 2013

A study on 4G network and its security

Sandeep Chouhan[1], R.B.Gaikwad[2], Neha Sharma[3]

Department of Electronics and Communication Engineering, Ujjain Engineering College, Ujjain M.P. (INDIA) [1, 2, 3]

Sandy24alive@gmail.com[1] , rambhaugaikwad@gmail.com[2] , nehatripathi@yahoo.com[3]

Abstract **With increasing user demands for wider service due to rapid growth & variety of IT (information technology) industry, the service with the data rate of 30 mbps cannot accommodate the future mobile multimedia environment. Therefore, with the advent 4th Generation communication system or 4G, there will be the certain path to the future radio and mobile communication system. In this paper, we will highlight the network structure, core network and technologies associated with the 4G. We also present the security architecture for 4G networks.**

Key-words: 4G network, NGN (next generation network), ITU-T X.805, IP network.

I. INTRODUCTION

As we know that the deployment of 3G is not completed yet and researchers interest shift towards beyond 3G i.e. 4th generation communication system or 4G . there is no formal definition for 4G but it shall provide a bandwidth of 100 Mbps in mobile and 1 Gbps in nomadic and it is all – IP with heterogeneous networks where multiple RATs (radio access technology) or RANs (radio access network) interoperate. Some of the basic enabling technologies for 4G are OFDM (Orthogonal Frequency Division Multiplexing), OFDMA (Orthogonal Frequency Division Multiple Access), and vertical handover protocols. Also, some advanced may include MIMO (Multiple Input Multiple Output), reconfigurable systems and cognitive radio or network. Some applications of 4G may include voice over IP (VoIP), MoD (Multi-Media On Demand), gaming and in general broadband wireless mobile internet services.

4G essentially builds an open environment where various network operators and service providers share the core infrastructure via open hardware and software platforms. This openness of 4G poses much more security challenges as opposed to the traditional closed environment (e.g. PSTNs) that has an inherent advantage of protection against security threats. It would just be a matter of time before 4G networks start to suffer the equivalent level of attacks experienced today by the current generation internet if the security issues couldn't be fully addressed. Hence, guaranteeing high level of security turns out to be one of the important requirements in the successful deployment of 4G networks.

Besides technical reasons, the network and service providers must ensure their infrastructures and services to be adequately protected against all kind of threats, as well as provide end users with secured accesses or services. This means they are required to 'secure' their network infrastructure for successful commercialization of their multimedia services. Accordingly, the need for secure networks and services will continue to grow as security will soon become a key differentiator for them.

The main contributions of this paper are:

- To oversee the historical evolution of the Mobile communication network in table no. 1 and
- To pinpoint the security architecture for 4G networks.

The rest of this paper is organized as follows. Section II presets an overview of network architecture for 4G networks. While section III describes the security architecture for 4G networks. In section IV we briefly explain ITU X.805, while the threat analysis for 4G networks is given in section V. In the last this paper concludes with section VI.

TABLE 1 Mobile Communication History

Property	1G	2G	2.5G	3G
Starting Time	1985	1992	1995	2002
Driven Technique	Analog signal processing	Digital signal processing	Packet switching	Intelligent signal processing
Representative standard	AMPS,TACS,NMT	GSM,TDMA	GPRS, I-Mode,HSCSD,EDGE	IMT-2000 (UMTS,WCDMA,CDMA2000)
Radio Frequency (HZ)	400M-800M	800M-900M,1800M-1900M	800M-900M,1800M-1900M	Same as 2G
Bandwidth (bps)	2.4K-30K	9.6K-1.4K	171K-384K	2M-5M
Multi-address Technique	FDMA	TDMA, CDMA	TDMA, CDMA	CDMA
Cellular Coverage	Large area	Medium area	Medium area	Small area
Core Networks	Telecom networks	Telecom networks	Telecom networks	Telecom networks, some IP networks
Service Type	Voice Mono-service Person-to-person	Voice,SMS,Mono-media Person-to-person	Data service	Voice ,Data, Some Multimedia Person-to-machine

II. NETWORK ARCHITECTURE

A. Network structure

4G will deploy single global cell core network to replace the cell network of 3G. Full IP will be applied in the network just like figure 1. Core network can support different access method just like IEEE 802.11a, WCDMA, Blue Tooth, HyperLAN. At the same time, the user device have the exclusive recognizable code, which can co-operate among isomerism system via hierarchies structure. The structure can make multiple services connect to IP core network transparently and have better commonality and extensibility.

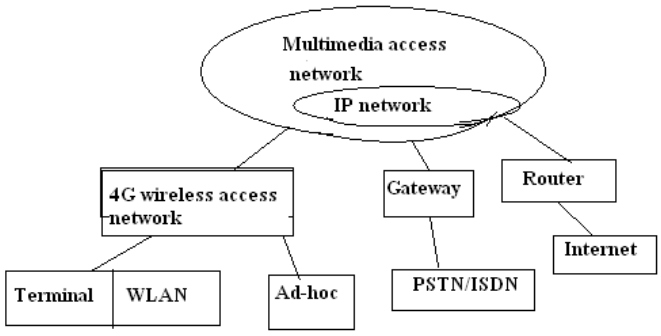

Figure 1 4G Network structure

B. Core network

4G mobile communication system is a full IP network. It has load mechanism based on IP, network maintenance and management based on IP, control of network source based on IP application services based on IP and etc.

Core network is independent of concrete wireless access network, can supply end-t-end IP service and can be compatible with current core network and PSTN. Core network have open

structure, can differ service/control/transport. Based on IP, the wireless access method and protocol is independent from core network, protocol and link layer. IP is compatible with more than one wireless access protocol, so it is very flexible when designing the core network and does ot need to take into account which method or protocol should be used in wireless access.

C. Mobile terminal

Future 4G mobile terminal should have following features:

- More strong interaction performance (more convenient connect to network)
- More high network connectivity (mobile device can build up by ad- hoc)
- Plenty of individuation service (can support cell phone, GPS location and etc.)
- Individuation, self – reconstruction ability (can change service demand ad network condition adaptively)
- Enhance security guarantee
- Enhance speech recogn0ition function

Moreover, 4G system can satisfy the requirements of high data rate and wide bandwidth. The terminal also must assure it can gear to different air interface and different QoS label ad mobility. To make compatible with different air interface, mobile terminal must have software refresh ability.

D. Core technique

In 4G, the core technology is OFDM. Future wireless multimedia service have high demand o both data transport and the transport quality. So the modulation technique must have higher cell rate as well as longer code element periodic.

OFDM is the short for Orthogonal Frequency Division Multiplexing, an FDM modulation technique for transmitting large amounts of digital data over a radio wave. OFDM works by splitting the radio signal to multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver. OFDM reduces the amount of crosstalk in signal transmissions. 802.11a WLAN, 802.16 and WiMAX technologies use OFDM.

Besides OFDM, there is W-ODFM technique, which enables data to be encoded on multiple high speed radio frequencies concurrently. This allows for greater security, increased amounts of data being sent, and the industries most efficient use of bandwidth. W-OFDM enables the implementation of low power multipoint RF networks that minimize interference with adjacent network. This enables independent channels t operate within the same band allowing multipoint networks and point-to-point backbone systems to be overlaid in the same frequency band.

III. 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 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 service scenarios;
- Usability that makes it easy for the end-users to users to use the security-enabled services;
- QoS guarantee that requires security solutions like cryptographic algorithms to meet QoS constraints of voice and multimedia traffic; and
- Cost- effectiveness that minimizes the additional cost of security and makes it lower than the cost of risks.

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 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.

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. 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.

The InMS security relias on the IPsec Encapsulating Security Payload (ESP) in tunnel mode to provide security features and Internet Key Exchange (IKE) to negotiate, establish and maintain keys.

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.

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 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 specific Security Gateways (SEGs) that enforce security policy between domains.

IV. ITU-T X.805 STANDARD

Network security and reliability becomes top issues for service providers and users. In spite of the importance, threats to cellular system may happen in any layers such as services and infrastructures as well as any planes such as user and management. Because it is complex to analyze security of

network systems, ITU developed the X.805 standard as a systematic analysis tool based on the Bell labs Security Model. By employing a modular approach, the X.805 builds a structured framework that effectively drives consideration of all possible threats and vulnerabilities for end to end network security. Moreover it provides a comprehensive, multilayered, end to end network security framework across eight security dimensions in order to combat network security threat.

In X.805, the network security is, as shown in figure 2 analyses by three layers (application, infrastructure, services) three planes (end user, control, management) and dimensions (access control, authentication, non reputation, data confidentially, communication security, data integrity, availability and privacy) to find any possible threats and or attacks of destruction, corruption, removal, disclosure, interruption.

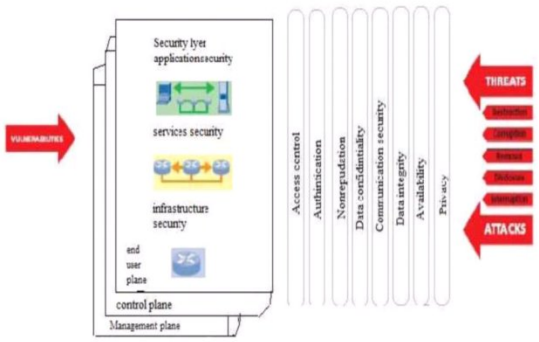

Figure 2: X.805 Network Security Analysis

Three security layers are 1) infrastructure layer that concerns individual communication links and network elements to securely create and maintain network, services and applications 2) service layer that deal with access service for instance, WiMAX access service that end users receive from networks , and 3) application layer in which applications for the end user via network interacting with remote hardware and software in order to access a information or perform a transaction example email, VPN etc

Security planes the three security planes are classified by the types of activities performed over the network management, control, and end user activity.

Security dimensions eight security dimensions look into measures implemented to counter threats and potential attacks. Access control measures protection level against unauthorized use of network resources authentication measures confirmation level for the identities of each entity using the network, Non-repudiation is to prove the origin of the data or identifies the cause of an event or action; Data confidentiality is to ensure that data is not disclosed to unauthorized users; Communication security is to allow information to flow only between authorized endpoints; Data integrity is to ensure the accuracy of data so it cannot be modified, deleted, created or replicated without authorization, and also provides an indication of unauthorized attempts to change data; Availability is to ensure that there is no denial of authorized access to network elements, stored information, information flows, services and applications due to network-impacting events Privacy is to provide for the protection of information that could be derived from the observation of network activities.

Nine modules are defined by three planes and three layers and each module is analyzed using the eight security dimensions. The security dimensions of different modules have different objective and consequently comprise different comprehensive sets of security measures. The basic methodology for analysis is to consider the threat model for each module and evaluate the effectiveness of security measures in each dimension.

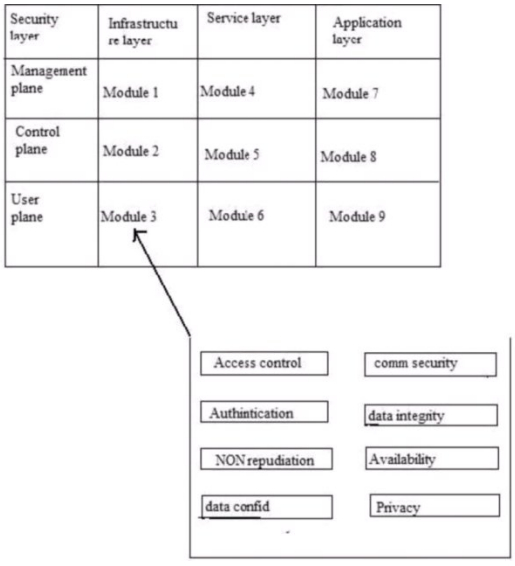

Figure 3: X.805 Modular Approach

V. SECURITY THREATS ON 4G

Possible security risks mostly arise from the open nature of 4G as summarized next. First of all, a large number of external

connectivity points with peer operators, with third-party applications providers, and with the public Internet, as well as numerous heterogeneous technologies accessing the infrastructure, serve as potential security holes if the security technologies do not fully interoperate. Moreover, multiple service providers share the core network infrastructure, meaning that compromise of a single provider may result in collapse of the entire network infrastructure. Finally, service theft and billing fraud can take place if there are third-parties masquerading as legitimate ones.

New end-user equipments can also become a source of malicious (e.g, DoS) attacks, viruses, worms, spam mails and calls, and so on. In particular, the Spam over Internet Telephony (SPIT), the new spam for VoIP, will become a serious problem just like the e-mail spam today. For example, SPITs targeting VoIP gateways can consume available bandwidth, thereby severely degrading QoS and voice quality. Clearly, the open nature of VoIP makes it easy for the attackers to broadcast SPITs similarly to the case of spam emails. Other possible VoIP threats included : (1) spoofing that misdirects communications, modifies data, or even transfers cash from a stolen credit card number, (2) SIP registration hijacking that substitutes the IP address of packet header with attacker's own, (3) eavesdropping of private conversation that intercepts and crypt-analyzes IP packets, and (2) phishing attacks that steal user names, passwords, bank accounts, credit cards, and even social security numbers.

VI. CONCLUSION

In this paper, firstly we discuss network architecture core technology of 4G mobile system and security architecture and then made comprehensive threat analyses to characterize the known (or possible) risks to each of them. Our threat analyses indicated that most of the IP-specific security vulnerabilities and threats will likely exist in 4G because 4G itself is an IP-based network. This means 4G will face much stronger security threats than those of current-generation networks. The 4G mobile system has high data rate, high spectrum utilization ratio, low transmitting power, supporting flexible services, so it will be certain path to the future radio and mobile communication system.

REFERENCES

[1] Li Weiwei, Comparison and Transition of Key Technologies on 3G and 4G, GUANGDONG COMMUNICATION TECHNOLOGY, 2004

[2] Zhand Jian, The Development Trends of 4G Technology, GUANGDONG COMMUNICATION TECHNOLOGY, 2004

[3] Jun-zhao Sun, Features in Future : 4G Visions from A Technical Perspective [C] IEEE Global Telecommunication Conference 2001. Vol 6.

[4] V.Gazis, "Evolving Perspectives of 4th Generation Mobile Communication Systems," IEEE PIMRC 2002, Coimbra, Portugal, Sept. 2002.

[5] T.B. Zhariadis et al., "Global Roaming in Next-Generation Networks," IEEE Commun. Mag., No. 2 Feb. 2002, pp. 145-51.

[6] Muxiang Zhang Yuguang Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," IEEE Transactions on Wireless Communication, vol. 4 Issue 2, 2005.

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

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

[9] E.F. Casas and C.Leung, "OFDM for data communication over mobile radio FM channels-part I: Analysis and experimental results," IEEE rans. Commun. Vol. 39, pp. 783-793, May 1991.

[10] Joi Woon Chong, Banf Chul Jung, and Dan Keun Sung, "Statistical multiplexing-based hybrid FH-OFDMA system for OFDM-based UWB indoor radio access networks," IEEE Transactions on Microwave theory and Techniques, Volume 54, Issue 4, Part 2, pp. 1793-1801, June 2006.

[11] Jun Zheng and B.D. Rao "LDPC-coded MIMO systems with unknown block fading channels : soft MIMO detector design, channel estimation, and code optimization," IEEE Transactions on Signal Processing Volume 54, Issue 4, pp. 1504, April 2006.

[12] R.W. Thomas, D.H. Friend, L.A. DaSilva, A.B. Mackenzie, "Cognitive networks: adaptation and learning to achieve end-to-end performance objectives, " IEEE communication Magazine, Volume 44, Issue 12, pp. 51-57, Dec 2006.