COMPREHENSIVE SURVEY OF POSSIBLE SECURITY ISSUES ON 4G NETWORKS

Sumant Ku Mohapatra[1], BiswaRanjan Swain[1] and Pravanjan Das[1]

Department of Electronics & Telecommunication Engineering, Trident Academy of Technology, Bhubaneswar,Odisha, India
Ericson Global private limited, Kolkata, India

ABSTRACT:

This paper presents a brief study of recent advances in wireless network security issues. The paper makes a number of contributions to the wireless networking field. First, it studies the 4G mail threats and risk and their design decisions. Second, the security of 4G architecture with next generation network security and 8-security dimensions of 4G network. Third, security issues and possible threats on 4G are discussed. Finally, we proposed four layer security model which manages to ensure more secure packets transmission by taking all the necessary security measures.

KEYWORDS

Network security, Security architecture, 4G, 3GPP, WiMAX, Threats

1.INTRODUCTION

The recent advances in wireless network technologies and the rising applications as web 2-0, mobile TV and streaming content led to the standardization of the 3rd generation partnership project (3GPP). The next generation wireless communication systems world wide standardized as 4G which has increased security and very much reliable communication. In terms of architectural design 4G is more interoperability across the HetNet environments and also it is operate on the TCP/IP architectural design procedure[3].When 3rd generation communication is moving to the 4th generation communication, many organizations are repairing for their 4G such as IEEE802.16m, International Telecommunication union (ITU), Vodafone, China mobile communications and many next generation mobile network vendors like Motorola and Samsung[2]. Now a days many definitions of 4G arises which provides a bandwidth of 1000 Mbps in mobile equipment and in normal 1Gbps. It is surrounding with heterogeneous networks having number of Radio Access Technology and Radio Access network[1]. The enabling technologies which is interconnected for 4G are orthogonal frequency division multiplexing, vertical handover protocols and in advance multiple input and multiple output and cognitive radio network are also included. Table 1 shows main threads and risk and design decisions of 4G is given below.

DOI : 10.5121/ijnsa.2015.7205 61

Table-1-4G Main threats and risk and their design decisions

Main threats and risk	4G design decisions
• Threats against user identity and privacy. • Threats related to base stations and handovers. • Threats related to broadcast or multicast signaling. • Threats related to denial of service. • Threats against manipulation of control plane data. • Threats of unauthorized access to the network. • Compromise of eNB credentials as well as physical attacks on the eNB. • Protocol attacks on an eNB. • Attacks on the core network.	• Permanent security association • New key hierarchy in evolved packet system. • Need for mutual authentication mechanisms. • Trusted environment and secure execution. • DOS protection of network • User privacy • Authorization

This paper studies different security issues and challenges in 4G technologies in section 3. The Remainder of this paper is organized as follows. Section 2 discuss 4G network technology architecture[7].Section 4 proposed a four layer security model which manages to ensure more secure packet transmission by taking all the necessary security measures such as taking the form of intrusion detection systems, Firewalls and IPsec and manipulating network resources in an intelligent manner using sophisticated authentication protocols.

2. 4G NETWORK ARCHITECTURE

The 4G network architecture is combination of multiple heterogeneous networks such as WiMAX and 3G[8]. Among the multiple access networks, anyone can used by the service subscriber and also it provides services from the same service unit like the IP Multimedia subsystems. Figure 1 shows aIMT-advanced 4G network system specified in ITU.

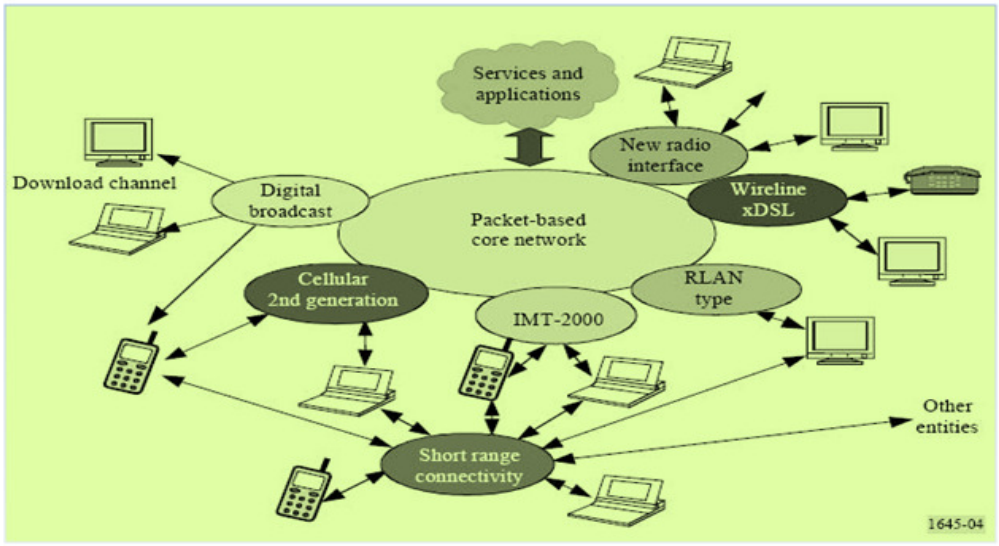


Figure 1: IMT-advanced 4G network system specified in ITU

The Wimax architecture has an access serving network to provide the service stations or mobile stations which is a connection to network service provider. But the 3GPP LTE architecture has two core networks such as GPRS and EPC network. The GPRS core network offer network connections for existing RANs and Evolved packet core network to give network connections to evolved RAN and 3 GPP IP Access.

2.1 IP Multimedia subsystem security architecture

The IMS (IP Multimedia subsystems) is an important overlay on top of the network infrastructure like 3 GPP. It aims to protect the all IMS sessions in between the end-users and IMS servers. It also offering it's authentication and authorization mechanisms. There are two parts of IMS security and are described below.

- First-hop Security: It secures the first hop from the end-user to the proxy-call session control function.

- Network domain security: It protects the rest of hops between call session control functions inside IME core.

2.2 Next Generation network security architecture

The next generation network security mostly secures the IMS security. It divided in to two security domains.

- Access view security: it secures the first hop for the end-user device to access the network.

- Core view security: It covers security within intra operated domain.

2.3 8-Security dimensions of 4G Network

The 8-security dimensions take care to measures implemented to counter threats and potential attacks.

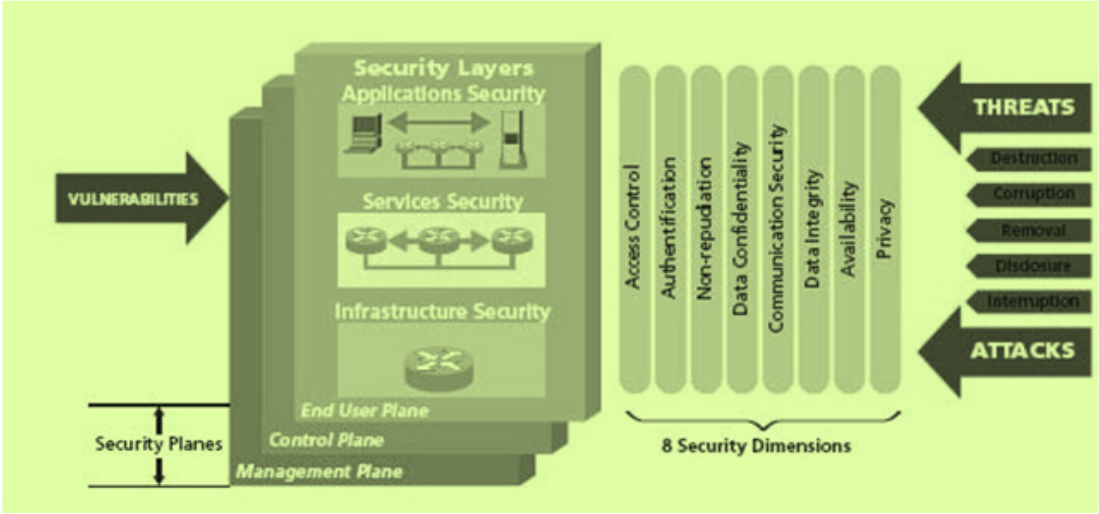


Figure 2: 8-Security dimension analysis

- Access control which measures protection level against unauthorized use of network resources.
- Authentication which measures confirmation level for the identities of each entity using the network.
- Non-repudiation which 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 end points.
- Data integrity is to ensure the accuracy of data so it can be modified, deleted, created or replicated without authorization and also provides an indication of unauthorized attempts to change the 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.

3. 4G WIRELESS SECURITY ISSUES

3.1 Physical layer issues

Both WIMAX and LTE are subject to two key vulnerabilities at the physical layer. By deliberately inserting man-made interference on to 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 (ii) multicarrier. 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 on to those carriers[4]. 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[1]. In addition, increasing the power of the source signal and using spreading techniques can increase it's resilience against interference. While the possibility of interference is significant, since it is easy to detect and address, we believe it's impact on the WIMAX/LTE network and users will be limited[13].

3.2 WiMAX-MAC-Layer security issues

To establish initial access with base station then IEEE802.16[11] Radio interface standard describes several steps in order for a mobile station, that includes seven steps.The steps are initial ranging and time synchronization, upper level parameter acquisition, basic capabiliiities negotiation, scanning and synchronization, mobile station authorization and key exchange, registration with the serving base station and the last step by which connection established. Among these steps five step involved non secure traffic and two other two steps involved secure traffic exchange based on the device authentication standards of Wi-max[6].

3.3 Denial of service security issues

The DoSattack are a concern for Wi-max network. These attack can be initiated through simple flooding attacking on authenticated management frames[2].

3.4 Wi-Fi security issues

Wireless LANs based on WI-FI technology have been available for more than a decade. However, the WI-Fi technology has most often been used in homes and public places such as airports, hostels, and shopping malls where security is seeming less critical, although the cost benefits of Wi-Fi could be attractive to enterprise environments thanks to increased mobility, lower operational costs, and flexibility. Accordingly, security researchers have focused on security threats and solutions in Wi-Fi networks to make it applicable to the enterprise

environments. The original security mechanism of Wi-Fi called wired equivalent privacy (WEP), had a number of security flaws arising from the mis-application of cryptography, e.g. the use

of RC4 stream cipher and CRC-32 authentication[3]. Regarding this, a comprehensive security evaluation based on the ITU-T X.805 standard has been performed[9].To remedy the security flaws of Wi-Fi, several solutions have been proposed. The Robust Security Network (RSN) for the IEEE 802.Ix standard's port based network access control is a layer-2 authentication mechanism and specifies how EAP can be encapsulated in the Ethernet frames. RSA Laboratory and Cisco have developed TKIP to mitigate the weakness of RC4 via frequent renewal of encryption key[5].

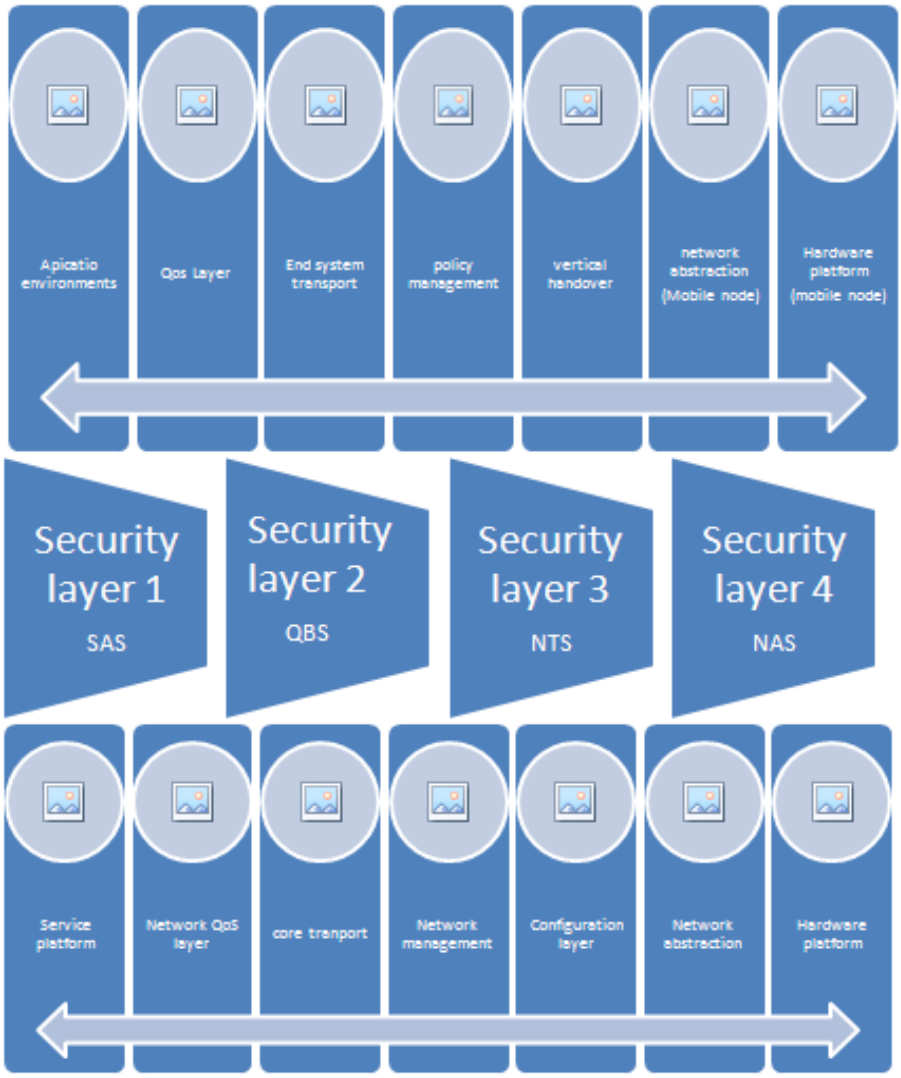
3.5. Possible Threats on 4G

The 4G may face lot of possible security Risks. The various heterogeneous technologies access the infrastructure, so potential security needed to secure technologies . Also it may collapse of the entire network infrastructure when multiple service providers share the core network infrastructure. In 4G wireless , end-user equipments can also become a source of malicious attacks worms, viruses, calls and spam mails and so on. The spam over internet, the new spam for VoIP results a serious problem like the today's E-mail spam[2]. As like the above VoIP threats other 3 more VoIP Threats are (1) spoofing that misdirects communications, modifies data, or transfers cash from a stolen credit card number. (2) Standard input point registration hijacking that substitutes the IP address of packet header with attacker's own. (3)Dropping of private conversation that intercepts and CRYPT arises IP packets.

4. PROPOSED 4G FOUR LAYER SECURITY MODEL

The proposed 4 layer security model integrated into the two frameworks, peripheral and core which allows to explore new security concepts. In this model 3 separate security layers such as network architecture security, network transport security and service and application security are used. It is designed to provide coherent heterogeneous communication on a global scale and it also provide continuous connectivity through the seem less operation of multiple mobile networks. These are accessible by mobile nodes, providing features like cognitive radio and vertical handover.

Peripheral network



Core network

Figure 3-Proposed four layer security model which is integrated in to the two frameworks

In this proposed model two frame works are used.

- Peripheral frame work which runs on the mobile node and interacts with wireless access networks.
- Core framework which runs in a distributed fashion in the core infrastructure.

By this double organized frame work, a multi layer security system arises that interacts with those two frameworks to provide a secure environment.

5. CONCLUSION

To better understand the security of 4G network we represent their different security accepts like physical layer issues, WiMAX-MAC layer issues, QoS issues and 4G Wi-Fi security issue. This study also discussed 8-security dimension of 4G network and represent possible threats on 4G. By the proposed four layer security model we try to avoid unsecureness of next generation wireless communication.

REFERENCES

[1] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," Proceedings of ACM MobiCom'2001, Rome, Italy, July 2001.

[2] T. Park, H. Wang, M. Cho, and K. G. Shin, "Enhanced Wired Equivalent Privacy for IEEE 802.11 Wireless LANs," CSE-TR-469-02,University of Michigan, November 2002, available from http://www.eecs.umich.edu/techreports/cse/02/CSE-TR-469-02.pdf.

[3] Bell Labs, "The Bell Labs Security Framework: Making the Case for End-to-End Wi-Fi Security," 2006.

[4] IEEE Draft 802.1x/D1, "Port Based Network Access Control," available from http://www.ieee802.org/1/mirror/8021/docs99/PortNACIEEE.pdf.

[5] I.S. Comsa et al., "Reinforcement Learning Based Radio Resource Scheduling in LTE-Advanced," Proc. 17th Int'l Conf. Automation and Computing (ICAC 11), IEEE, 2011,pp. 219–224.

[6] J. Berkmann et al., "On 3G LTE Terminal Implementation—Algorithms,ComplexitiesAnd Challenges," Proc. Int'l Wireless Communications andMobile Computing Conf. (IWCMC 08), IEEE, 2008; doi:10.1109/IWCMC.2008.168

[7] Z. Shi et al., "Layered Security Approach in LTE and Sim-ulation," Proc. 3rd Int'l Conf.Anti-counterfeiting, Security,and Identification in Communication (ASID 09), IEEE,2009;doi:10.1109/ICASID.2009.5276930.

[8] C. Vintila, V. Patriciu, and I. Bica, "Security Analysis of LTE Access Network," Proc.10th Int'l Conf. Networks (ICN 11), Int'l Academy, Research, and Industry Assoc.,2011, pp. 29– 34.

[9] Network Architecture, tech. specification 3GPP TS 23.002 V9.1.0, 3GPP, 2009.

[10] D. Forsberg, LTE Security, John Wiley, 2013.

[11] H. Mun, K.Han, and K. Kim, "3G-WLAN Interwork-ing: Security Analysis and New Authentication and Key Agreement Based on EAP-AKA," Wireless Telecommunications Symp.(WTS 2009), IEEE, 2009; doi:10.1109/ WTS.2009.5068983.

[12] N. Seddigh et al., "Security Advances and Challenges in 4G Wireless Networks," Proc..8th Conf. Privacy Security and Trust (PST 10), 2010,IEEE; doi:10.1109/PST.2010.5593244

[13] L. Huang et al., "Performance of Authentication Protocols in LTE Environments,";Proc.Int'l Conf. Compu-tational Intelligence and Security (CIS 09), IEEE, 2009. doi:10.1109/CIS.2009.50

[14] L. Hui and B. Shuo, "Research and Implementation of LTE NAS Security," Proc. Int'l . doi:10.1109/ICEIT.2010.5607551

[15] 3G Security: Security Threats and Requirements, tech. specification TS 21.133, 3GPP,2001. Conf. Educational and Information Technology (ICEIT 10), IEEE, 2010;

Authors

Sumant Ku Mohapatra is working as Assistant Professor in Trident Academy of Technology, Bhubaneswar affiliated to B.P.U.T, Odisha, India. His research interests include wireless communication, digital signal processing, image processing and optical fiber communication

BiswaRanjan Swain is working as Assistant Professor in Trident Academy of Technology; Bhubaneswar affiliated to B.P.U.T, Odisha, India. His areas of research interests are in satellite & wireless communication, digital image processing and optical fiber communication .

Pravanjan Das worked in Trident Academy of Technology, B.P.U.T, Bhubaneswar, Odisha, India as an Assistant Professor. His research interest is in wireless communication. Now he is working in Ericsson India Global Services Pvt. Ltd, Kolkata, India