Journal of Advances in Science and Technology
Vol. 12, Issue No. 25, (Special Issue) December-2016, ISSN 2230-9659

Security Threats and Security Issues in 4G Wireless Network

S. V. Manjaragi[1]*, S. V. Saboji[2]

[1]Department of Computer Science and Engineering, Hirasugar Institute of Technology, Nidasoshi, Karnataka, India

[2]Department of Computer Science and Engineering, Basaveshwar Engineering College, Bagalkot, Karnataka, India

Abstract – 4G is the next generation of wireless networks that will totally replace 3G networks. It will provide better speed and fully IP based multimedia services. 4G is all about an integrated, global network that will provide voice, data and streamed multimedia services to users on "Anytime, Anywhere" basis. The important and challenging issue in 4G is seamless handoff, mobility management, security and service between different integrated networks.

This paper surveys security requirements, challenges, security threats and different 4G networks security architectures. It also discusses 4G security techniques and security issues. Specifically we discuss about Y-Comm security models for heterogeneous networks, Hokey Project, and ITU X.805 framework. It also describes security issues with physical layer, MAC layer, Key Management pertaining to integrated WiMax, WiFi, and 3G LTE networks.

Our survey shows that a number of new security threats to cause unexpected service interruption and disclosure of information. We also found still there are several open security issues and challenges although many are working on fixing and designing new security architectures for 4G.

Keywords— 4G Security architecture, 4G Security threats and Challenges, 4G Security Issues

----------♦----------

INTRODUCTION

The fourth generation (4G) networks is integration of many existing access networks such as 3G, LTE, WLAN (Wi-Fi), Wi-Max, and satellite communications where users are always connected. It is providing voice and data transfer with high quality-of-service (QoS), and is intended to provide high speed internet access to support voice/video multimedia applications.

4G networks provides an open environment where different service providers with different wireless technologies share an IP-based core network to provide uninterrupted services to their subscribers with the same quality of service (QoS) [1]. In 4G systems, mobile equipments are switching from one network to another of different operators and wireless technologies; this is known as vertical handover. All these elements providing loop holes in security and vulnerabilities. Due to the open nature and IP-based infrastructure for 4G wireless, attention needs to be given to understand and study the security threats and issues. The task of securing 4G wireless networks and systems is a challenging one.

The main security concerns [2] of a 4G network includes, first, Securing hardware, software, data and operating System known as Application Security, second, Confidentiality Integrity Authentication and Authorization (CIAA) of data known as Network access security, and User's Identity, Confidentiality and authorization known as User security [3].

This paper presents a comprehensive survey of 4G Networks security requirements, challenges, possible/known security threats, 4G security architectures, security techniques and security issues. The main contributions of this paper are, first, to understand the 4G Security requirements and challenges, second, and to study and analyze the different 4G security possible security threats and security architectures, and then analyze the existing security techniques used for securing 4G networks and security issues on 4G wireless networks. The rest of this paper is organized as follows; Section 2 presents an overview security requirements and challenges, while section 3 describes possible 4G Security threats and attacks, section 4 describes of

security architecture for 4G Networks and section 5 describes security issues in 4G.

II. 4G SECURITY REQUIREMENTS AND CHALLENGES

The main concern of any wireless mobile device is security with respect to data, hardware, user's identity and privacy. Security flaws are initiated either by the attacker or because of incorrect network or user's mobile parameter settings. For e.g., if user's mobile settings are kept open, any attacker can access the data, and in another scenario even after having good security features of the device, signaling at12tack can lead to resource exploitation. In these cases, the affected mobile user will be denied access even the resources such as channel, bandwidth, energy are available. Thus in 4G systems it is required to add security features that can balance the resource availability while achieving high QoS.

The security requirements of 4G heterogeneous networks have been defined on two levels: firstly, these are on mobile equipment; and, secondly, on operator networks. Mobile equipment requirements include protecting the device's integrity, privacy and confidentiality, controlling access to data, and preventing the mobile equipment being stolen. Existing research on security of 4G heterogeneous networks focused on the security such as authentication and authorization that is on the interface between the network and the operator.

Security issues in mobile computing are now presenting many challenges. The ability to move from one network to another, and from one provider to another creating thus vertical and horizontal handoffs, has increased the complexity of mobile security. Therefore, it is necessary to design security solutions which are independent from the network, provider, and end user devices. The protection should involve not only data but, also an entity that is 4G should protect both the entities and infrastructure. The network and service providers must ensure their infrastructures and services are protected against all kinds of threats, as well as provide end users with secured accesses/services.

III. 4G SECURITY THREATS AND ATTACKS

4G networks represent an open environment where different wireless technologies and service providers share an IP-based core network to provide uninterrupted services to their subscribers with almost the same quality of service (QoS). Due to the open architecture and IP based environment, 4G heterogeneous networks receive new security threats and derive threats from the internet. There are many possible threats within a 4G network system. These threats are: [4] IP address spoofing, User ID theft, Theft of Service (ToS), Denial of Service (DoS), and intrusion attacks. New threat in 4G not seen in 3G the network infrastructure was owned by the service providers and access was denied to other network equipment.

In mobile communications, another security problem is when the end user device is disconnected from the network because of no power in the battery. When device is switched on it will go from level of disconnection to connection presents an opportunity for the attacker to show himself as a mobile device or a mobile support station.

In addition, new end user devices are sources of denial of service attacks, viruses, worms, and so on. The security threats according to X.805 are destruction, corruption modification of information, theft, removal or loss of information, disclosure of information, and interruption of services.

Protocol specific attacks include malformed message attacks, buffer overflow attacks, Denial-of-Service (DoS) attacks, RTP session hijacking, and insertion of unauthentic RTP. 4G Networks can be viewed as convergence of networks such as Wi-Fi, WIMAX, and LTE. 4G will inherit all the security problems of 4G's access networks (such as 3G cellular networks, LTE, Wi-Fi, Wi-Max networks, sensor networks and so on). Therefore we need to do security analysis of these standards.

A. WI-FI SECURITY THREATS

Wireless LANs based on Wi-Fi technology (IEEE 802.11) has been used in homes, cafes, airports, hotels and shopping malls where security is less important. Because of its cost benefits such as increased mobility, lower deployment/operational costs, and flexibility Wi-Fi is attracting but it has some serious security threats. The original security mechanism of Wi-Fi, called Wired Equivalent Privacy (WEP), had a number of security flaws [5]. To solve these security flaws of Wi-Fi, several solutions have been proposed the Robust Security Network (RSN) [6] for the IEEE 802.1x standard's port based network access control is a layer-2 authentication mechanism and specifies how EAP can be encapsulated in the Ethernet frames. LEAP [7] aims to support mutual authentication between a mobile terminal and the AP, thereby defeating man-in-the-middle attacks.

B. WI-MAX SECURITY THREATS

WiMAX addresses the compatibility and interoperability of broadband wireless access products using the IEEE 802.16 standards consisting of IEEE 802.16-2004 and 802.16e-2005 mobile architectures. IEEE 802.16-2004 defines a Privacy Key Management (PKM) protocol by which Mobile Station (MS) authenticates itself, obtains Authorization Key (AK) from the Base Station (BS), and derives other keys like Key Encryption Key (KEK), Traffic Encryption Key (TEK) and so on. It also

supports two encryption algorithms, i.e. DES in CBC mode and AES in CCM mode.

Weaknesses of 802.16-2004: First, it is vulnerable to an attack from bogus BS since there's no mutual authentication between BS and MS. Second, the encryption keys are solely generated by BS instead of the two parties, MS and BS. Third, it does not support integrity protection of management frames, exhibiting a potential risk of denial-of-service (DoS) attacks.

In IEEE 802.16e-2005, an improved version of PKM is developed to fix known vulnerabilities of PKM. The improved PKM makes it mandatory to perform mutual authentication between MS and BS via RSA and/or EAP (Extensible Authentication Protocol). Although IEEE 802.16e-2005 corrected almost all of the security weaknesses of its precursor, it still suffers several security vulnerabilities; for instance, TEK is still chosen by BS while certificate management is not yet comprehensive.

C. 3GPP LTE SECURITY THREATS

The 2G uses Authentication and Key Agreement (AKA), its security is weak in that its authentication is only unidirectional; the user cannot authenticate the serving network. In 3GPP AKA, improved are the mutual authentication and agreement on an integrated key between the mobile terminal and the serving network, and the freshness assurance of agreed cipher key and integrity key. Although the 3GPP AKA has been accepted as reliable and used, there still exist weaknesses in 3GPP AKA [8]. The weaknesses include, redirecting user traffic using false BS and mobile terminals, given the fact that the counter value of set to a high value by adversary, the mobile terminal's life time may be shortened, because a home network keeps a counter and dynamically synchronized for every mobile terminal, a fault in counter database may affect all mobile terminals.

D. POSSIBLE THREATS ON 4G

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 affecting the 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 include, spoofing that misdirects communications, modifies data, or even transfers cash from a stolen credit card number, SIP registration hijacking that substitutes the IP address of packet header with attacker's own, eavesdropping of private conversation that intercepts and crypt-analyzes IP packets, and phishing attacks that steal user names, passwords, bank accounts, credit cards, and even social security numbers.

E. DOS ATTACK ON 4G NETWORKS

A DoS attack on a network is reducing the capacity of the network and disrupting communication. It reduces both the functionality and the overall performance causing inconvenience to both user and service provider. 4G is a heterogeneous network that consists of many wireless technologies from 2G to 3G to WLAN and WiMax. Each modulation technique suffers from jamming attack that can be the one way of DoS attack in the physical layer. Jamming attacks block the communication between the users's mobile device to the base station (BS). Jammer is a device, which can partially or completely disrupt a node's signal, by adding a noise to the signal. Jammer parameters such as signal strength, location and type influence the performance of the network and each jammer having a different effect on the user and the network. Jammer and interference caused by the cell allocation takes places in the physical layer; whereas in the routing layer, collision attack and signaling attack causes the system to either go to shutdown. In the transport layer, the possibility of flooding and authorization attack is high. In the application layer, authentication attacks are possible.

IV. SECURITY ARCHITECTURE FOR 4G NETWORKS

The security architecture for 4G systems should meet the security requirements such as increased robustness over 3G, user identity and confidentiality, strong authentication of user and network, data integrity, confidentiality and working of security across different radio networks. The objectives in designing the security architecture are to make network available for access all the time that is networks and services not to be interrupted by malicious attacks. Make it easy for the end-users to use the security-enabled services. International communication societies (IEEE, WiMAX, 3GPP, and ITU), research groups and researchers have proposed different security architectures for 4G networks, which include: Y-Comm security models for heterogeneous networks, Handover Keying working group (Hokey WG), and ITU X.805 framework.

A. Y-COMM SECURITY MODELS (IEEE 802.21) FOR HETEROGENEOUS NETWORKS

Y-Comm framework [9, 10] is new communication architecture proposed by University of Cambridge and is implemented in the Cambridge wireless testbed. This new Internet generation will provide continuous connectivity through the operation of multiple mobile networks. It has a four-layer security integrated module to protect data and three targeted security models to protect different network entities.

The Y-Comm architecture consists of two frameworks namely *Peripheral framework:* deals with issues in Peripheral Networks, and *Core framework:* deals with issues in the Core Networks.
The Y-Comm architecture is shown in Figure 1.

In this architecture, the Peripheral and the Core Frameworks are work together to represent a 4G networks which supports heterogeneous devices, different wireless networking technologies, network operators and service providers. To have total security Y-comm has a multi layer security model which should be applied to both Peripheral Framework and Core Framework simultaneously. The important point in this model is that, need to support heterogeneous networking with open architectures that is security should not only protect data but entities such as Application security, Network Access Security, and User Security.

The topmost layer of security called Service and Application Security (SAS). In the Peripheral Framework, SAS is used to authenticate users and applications; hence it defines the Authentication, Authorization, Auditing and Cost (AAAC) functions at the end-device. SAS in the Core network provides AAAC functions for services on the Service Platform in the core network. The next security layer is called QoS-Based Security (QBS) and is concerned with QoS issues and the changing QoS demands of the mobile environment for user mobility. The QBS layer also attempts to block QoS related attacks, such as Denial-of-Service (DoS) attacks on networks and servers.

The next security layer is known as Network Transport Security (NTS). In the Peripheral network, NTS is responsible for access to and from end-devices and services on the Internet. In the core network, NTS is used to establish secured connections through the core network. So NTS in the Core Framework involves preparing secure tunnels between core endpoints using IPsec mechanism to transfer the data in secured manner across the core network.

The fourth and last layer of this security model is called Network Architecture Security (NAS). In the Peripheral Framework, it tries to address security issues and threats involved in using particular networking technologies. So when a mobile device wishes to use any given network, NAS is invoked to ensure that the user is authorized. Further Y-Comm provides three network security models.

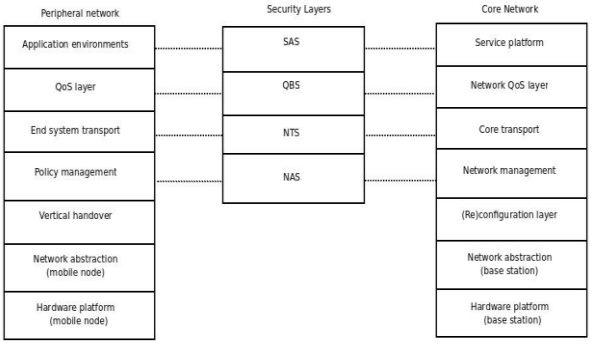

Fig.1: Y-Comm Architecture

*Connection Security Model***:** In this model, the different security layers work together to establish a connection between a mobile node and a service being hosted at another site. Interaction between mobile node and server is shown in Fig.2

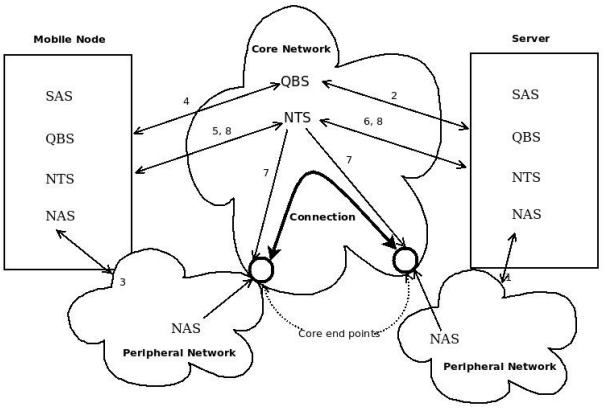

Fig. 2: Connection Security Model

B. HANDOVER KEYING WORKING GROUP (HOKEY WG)

The important operation of 4G wireless network is seamless vertical handoff; it is the process of transferring a live call or data session from one connected cell of the core network to another or one network to another. A mobile device must re-authenticate each time when it enters into the network. This is most time consuming task. In this process of re-authentication, it creates a series of security threats. Therefore it is required to minimize the time it takes to re-authenticate.

The Hokey WG [11] is currently undergoing research, developing techniques for faster key reuse and authentication. They have not yet defined the complete suite of protocols but proposed some solutions, authentication and key management take place before handoff. The main advantage is that authentication and key agreement does not need to be performed during handoffs. In the second approach, the reuse of ciphering material generated

during the initial authentication saves time during re-authentications.

The Hokey WG is trying to define an extended master session key (EMSK)-based technique for both authenticated and seamless handovers. This produced key is also known as the re-authentication Root Key (rRK). The rRK is used to derive the re-authentication Integrity Key and a re-authentication master session key (MSK) that is specifically associated to each authenticator. The first key mainly plays the role of proof validation between the peer and the AAA server, whereas the second is used to derive the access link security-key material after the re-authentication procedure.

C. ITU X.805 FRAMEWORK

International Telecommunication Union (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 [12, 2] builds a structured framework that considers all possible threats and vulnerabilities for end-to-end network security.

It provides a multilayered, end-to-end network security framework across eight security dimensions in order to address network security threats. In X.805, the network security is, as shown in Fig 3, analyzed by three layers (applications, services, infrastructure), three planes (end user, control, management), and eight dimensions (access control, authentication, non-reputation, data confidentiality, communication security, data integrity, availability, and privacy) to find any possible threats or attacks of destruction, corruption, removal, and interruption.

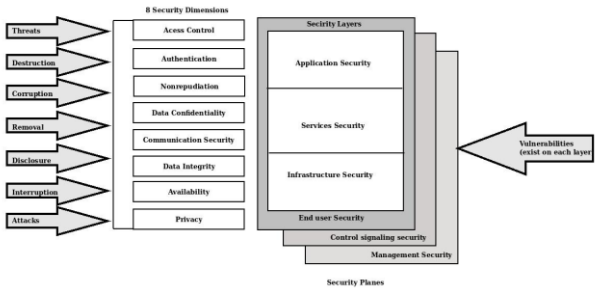

Fig. 3 ITU X.805 Security Model

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 services and 3) application layer in which application services for the end-user via network interacting with remote hardware or software in order to access information or perform a transaction e.g. 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. These include, *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 is 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 objectives.

V. 4G SECURITY ISSUES

The main security concerns of any wireless mobile securing data, hardware and user's privacy and integrity. Security flaws are initiated either by the attacker or due to incorrect device or network parameter settings. For e.g., user's mobile settings is often kept open, hence any attacker can access the data, and in another scenario where in spite of good security features of the device, constant signaling attack can lead to resource exploitation. In these cases, the mobile user will be denied access even the resources such as energy, channel, bandwidth are available. Thus 4G requires security features that balance the resource availability while achieving constant QoS.

The *security concerns* of a 4G network includes,

- *Application Security:* Integrity of the hardware, software, data and operating System (OS).

- *Network Access Security:* Confidentiality, Integrity, Authentication and Authorization (CIAA).
- *User security:* User's identity, Confidentiality and authorization.
- *Network area Security*: ME's location authentication and confidentiality.
- *QoS maintenance*: Security against Denial of Service (DoS) attacks to maintain constant QoS.
- *Physical Security*: Tamper resistance.

The security requirements of 4G heterogeneous networks have been defined on two levels: firstly, these are on mobile equipment; and, secondly, on operator networks. Mobile equipment requirements include protecting the device's integrity, privacy and confidentiality, controlling access to data, and preventing the mobile equipment being attacked and the data being abused or used as an attack tool.

Existing research on security of 4G heterogeneous networks focused on the security such as authentication and authorization that is on the interface between the network and the operator. However, the protection of the mobile device from attacks and becoming an attack tool solves important security issues in the heterogeneous network. The mobile security requirements such as protecting the mobile equipment; integrity of the hardware, and software. They do not prevent access to the mobile data and the mobile equipment can be used as an attack tool.

Security issues in mobile computing are now presenting many challenges. The ability to move from one network to another, and from one provider to another creating thus vertical and horizontal handoffs, has increased the complexity of mobile security. 4G networks are fully IP-based, and hence we can consider the security threats related to internet and IP security vulnerabilities. These new challenges are: IP address spoofing, user ID theft, Theft of Service, Denial of Service, and intrusion attacks. Therefore, it is necessary to design security solutions which are independent from the network, provider, and end user devices.

The protection should involve not only data but, also an entity that is 4G should protect both the entities and infrastructure. The network and service providers must ensure their infrastructures and services are protected against all kinds of threats, as well as provide end users with secured accesses/services. This means they are required to 'secure' their network infrastructure for successful commercialization of their multimedia services**.**

A. Physical Layer Issues

There are two vulnerabilities at the physical layer in WiMAX and LTE Interference and Scrambling attacks [13]. The attacker deliberately inserts interference onto a medium that causes high signal-to-noise ratio and hence, communication system may stop functioning. There are two types of interference that can be carried out: noise and 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 onto those carriers. Scrambling is another form of interference which is carried out for short intervals of time. The attacker may target specific frame, management or control information of a particular user to disrupt service. It is very difficult to detect the attacker.

B. MAC-Layer Security Issues

There are some issues related to MAC layer. Some of the issues related to WiMax and LTE are discussed.

WiMAX- MAC Layer Security Issues

The IEEE 802.16 radio interface uses 8 different steps in order for a MS to establish initial access with a Base Station. These steps are Scanning and Synchronization, UL Parameter Acquisition, Initial Ranging and Time Synchronization, Basic Capabilities Negotiation, MS Authorization and Key Exchange, Registration with the Serving BS, Connection Establishment. The first five steps involve non-secure traffic. Thus, they are prone to various attacks. At the MAC layer, WiMAX is susceptible to DoS attacks, eavesdropping, replay attack, service degradation, and vulnerabilities due to faulty key management.

Denial of Service (Dos): A DoS attacks can be done in many different ways. A DoS attack can be initiated by simple flooding, attacking unauthenticated management frames. The Subscriber Station/ Mobile Station (SS/MS) authenticate the BS using PKMv2 RSA authentication. In this scenario, the BS has to sign and reply with its public key. If flooded with false requests, the BS will be very busy computing and evaluating digital signatures and will be not able to serve any other requests. In a second case an adversary eavesdrops and captures the Authorization Request message from a particular SS to a BS.

The attacker then replays the captured message repeatedly. This will burden the BS which will then decline requests from other authentic SS devices. In a third case, unauthenticated management frames could be maliciously exploited by attackers.

Service Degradation: MAC Management messages are never encrypted and not always authenticated. This can lead to man-in-the-middle attacks causing service degradation. For example, (MOB_TRF-IND) is

an unauthenticated broadcast message. It is used by the BS to inform a sleeping MS that there is traffic destined to it. These messages can wakeup as many as 32 MSs. A falsely generated message can simultaneously drain the battery of up to 32 MSs.

Authorization Vulnerability: The authorization protocol is vulnerable to certain replay attacks in such a case, the attacker replays an instance of the Authorization Request message sent earlier. The BS then responds with an Authorization Reply message. The BS cannot ignore duplicates since it may be a legitimate duplicate request from the SS due to loss of the previous Authorization Reply message. The BS has to sign and reply with its public key. Processing of public key encryption and signature consumes CPU power. If flooded with replay attacks, the BS will be busy in computing and evaluating digital signatures. As a result, it will have little CPU power left to serve any other SS requests.

Security Issues with Key Management: Key management at the SS has been designed to protect it from replay attacks. The SS can determine if a Key Reply message is new or old. This is possible since the old TEK (Traffic Encryption Key) and new TEK are included in the Key Reply message. However, if an attacker replays Key Request messages to the BS, it can trigger frequent exchange of keying materials. This will cause confusion at the SS and exhaust resources at the BS. Another issue arises from the combination of the TEK lifetime and crypto algorithm deficiency. The TEK lifetime can be set to a value ranging between 30 minutes and 7 days. The data may be vulnerable if the TEK lifetime is set to a large value. A third issue involves key management in multicast and broadcast services. 802.16e uses common group traffic encryption key (GTEK) for traffic encryption/decryption. Each multicast group member must know this key. The transfer of GTEK to all groups is broadcast but encrypted with the shared key encryption key (SKEK). The issue of backward and forward secrecy is not addressed. When a new member receives the current GTEK, it can decrypt all previous messages that were multicast during GTEK's lifetime.

LTE – MAC Layer Security Issues

Security issues need to be addressed within LTE – categorized below into 4 key types.

Location Tracking: Location tracking means tracking the UE presence in a particular cell or multiple cells. Location tracking is made possible by tracking a combination of the Cell Radio Network Temporary Identifier (C-RNTI) with handover signals or with packet sequence numbers.

Bandwidth Stealing: The buffer status report is used as input information for packet scheduling, load balancing, and admission control. Sending false buffer status reports on behalf of another normal UE can change the behavior of these algorithms. By changing the packet-scheduling behavior at the eNB, it is possible to carry out a bandwidth stealing attack making the eNB believe that the UE does not have anything to transmit.

Security Issues Due to Open Architecture:

In LTE networks, there may be two possible ways to carry out DoS. The first type of DoS attack would be against a specific UE. A malicious radio listener can use the resource scheduling information along with the C-RNTI to send an uplink control signal at the scheduled time, thus causing a conflict at the eNodeB and service problems for the real UE. Type of DoS attack can be based on the buffer status reports used by an eNB for packet scheduling, load balancing, and admission control. Attackers can send reports impersonating a real UE. If the impersonator sends buffer status reports which report more data to send than are actually buffered by the real UE, this will cause a change in the behaviour of admission control algorithms. If the eNB sees many such fake buffer status reports from various UEs, it may believe that there is a heavy load in this cell. Consequently, the eNB may not accept newly arrived UEs.

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 a range of security attacks including for example Malware, Trojans and Viruses. Apart from end-user equipment posing traditional security risks, it is expected that new trends such as SPIT (SPAM for VoIP) will also become a security concern in 4G LTE and WiMAX. Other VoIP-related security risks are also possible such as SIP registration hijacking where the IP address of the hijacker is written into the packet header, thus, overwriting the correct IP address.

VI. CONCLUSION

To better understand the security of 4G networks, we studied the activities of international communication societies (IEEE, WiMAX, 3GPP, and ITU) with an emphasis on network security issues. We first summarized 4G security requirements, challenges, then made comprehensive threat analyses to

understand the known (or possible) risks/threats, understood the 4G security architectures proposed by different international communication societies and finally, discussed about security issues.

Our study on 4G security threats showed that 4G will inherit all the security problems of its access networks (such as 3G cellular networks, LTE, WiFi, WiMAX networks, etc.) because of their heterogeneous and open architecture, and IP-specific security vulnerabilities and threats are exist in 4G because 4G itself is an IP-based network. This means 4G will face stronger security threats than the current-generation networks. Hence, we have studied security threats of WiFi, WiMax, 3G LTE networks and 4G security threats including DoS attack.

Our study on 4G network security architecture shows that, there are two security approaches, first, multilayer and multidimensional network security architecture(Y-comm and X.805), second, mobility protocol and key management solution (Hokey project). Y-comm model is integration of the various layers into the security framework make it possible to design new security solutions. It will protect data and security models to target security on different entities and hence protecting not only the data but, also resources, servers and users. The handover keying working group (HOKEYWG) is currently working on a new mechanism to support inter-technology handover which deploys the Extensible Authentication Protocol (EAP) to support handover key distribution. This mechanism can be used to secure vertical handover model.

The study of security issues focused on MAC layer vulnerabilities for WiFi, WiMAX and LTE. These have some physical layer vulnerabilities to interference and scrambling techniques. At the MAC layer, WiMAX is susceptible to DoS attacks, eavesdropping, replay attack, service degradation. LTE also has a set of vulnerabilities at the MAC layer such as location tracking, DoS attacks and data integrity attacks.

Security development has no ending, new threats and attacks will. Hence, the comprehensive threat analysis and the development of appropriate countermeasure for the entire 4G systems must be made in parallel with the evolution of 4G architecture, which are on-going research. We feel that research with emulation and testbed related studies which will reveal further issues and challenges to be addressed.

REFERENCES

Mahdi Aiash, Glenford Mapp, Aboubaker Lasebae and Raphael Phan, “Providing Security in 4G Systems: Unveiling the Challenges”, AICT '10 Proceedings of the 2010 Sixth Advanced International Conference on Telecommunications, pp.439-444, May 2010.

ITU-T, “X.805: Security architecture for systems providing end-to-end communications”, 2003.

Zheng Y, He D, Yu W and Tang X, “ Trusted Computing-Based Security Architecture For 4G Mobile Networks”, Proceedings of 6th International conf on Parallel and Distributed Computing, Applications and Technologies (PDCAT 05), 2005.

Y. Park and T. Park, “A Survey of Security Threats on 4G Networks”, Proc*. Globecom Workshops*, IEEE, 2007.

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.

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

Cisco, “Lightweight Extensible Authentication Protocol (LEAP),” available from http://www.cisco.com/warp/public/102/wlan/nextgen.html

Muxiang Zhang Yuguang Fang, “Security analysis and enhancements of 3GPP authentication and key agreement protocol,” IEEE Transactions on Wireless Communications, vol. 4 Issue 2, 2005.

G. Mapp, D.N. Cottingham, F. Shaikh, P. Vidales, L. Patanapongpibul, J. Balioisian, and J. Crowcroft, “An Architectural Framework for Heterogeneous Networking”. International Conference on Wireless Information Networks and Systems (WINSYS), pp. 5-10. August 2006.

G.E. Mapp, F. Shaikh, D. Cottingham, J. Crowcroft, and J. Beliosian, “Y-Comm: A Global Architecture for Heterogeneous Networking” (Invited Paper), 3rd Annual International Wireless Internet Conference (WICON 2007), October 2007.

Anastasios N. Bikos, Nicolas Sklavos, “LTE/SAE Security Issues on 4G Wireless Networks” , IEEE Security & Privacy, Copublished by the IEEE Computer and Reliability Societies, March/April 2013.

Y. Park and T. Park, “A Survey of Security Threats on 4G Networks”, Proc*. Globecom Workshops*, IEEE, 2007.

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.

Corresponding Author

S. V. Manjaragi*

Department of Computer Science and Engineering, Hirasugar Institute of Technology, Nidasoshi, Karnataka, India

E-Mail – shiva_vm@rediffmail.com