A SURVEY OF 4G NETWORK SECURITY MODELS

S V MANJARAGI
Hirasugar Institute of Technology/Computer Science and Engineering, Nidasoshi, Karnataka, India
Email: shiva_vm@rediffmail.com

S V SABOJI
Basaveshwar Engineering College/Computer Science and Engineering, Bagalkot, Karnataka, India
Email: saboji_skumar@yahoo.com

C B AKKI
Professor, Department of ISE, SJB Institute of Technology Bangalore, India,
Email: akki.channappa@gmail.com

ABSTRACT: 4G communication network strive to seamlessly integrate existing heterogeneous wireless communication technologies and is fully IP-based wireless Internet which will provide access to wide range of mobile services. The challenging issue in 4G is seamless handoff, Mobility management, Security and Service between different integrated networks. This paper describes security requirements, challenges security threats, security architectures of 4G networks. Specifically, the paper describers Y-Comm security models for heterogeneous networks, Hokey Project, and ITU X.805 framework.

Our survey on 4G Security models shows that a number of new security threats cause unexpected service interruption and revelation of information. We also found still we need to work towards designing a new security architectures for 4G or enhancement in the existing architectures.

KEYWORDS: 4G Networks, 4G Security architecture, 4G Security threats and Challenges.

INTRODUCTION

The fourth generation (4G) networks is integration of many existing access networks such as 3G, LTE, LAN (Wi-Fi), WiMax, 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, security threats, and 4G security architectures. The main contributions of this paper are, first, to understand the 4G Security requirements and challenges, second, to study and analyze the possible security threats on 4G Networks and finally, study and analyzing the 4G security architectures, 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.

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 attack 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.

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, Real time Transport Protocol (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, Long Term Evolution (LTE), Wi-Fi, WiMAX networks, sensor networks and so on). Therefore we need to do security analysis of these standards.

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 IEEEs 802.1x standard's port based network access control is a layer-2 authentication mechanism and specifies how Extensible Authentication Protocol (EAP) can be encapsulated in the Ethernet frames. Lightweight Extensible Authentication Protocol **(**LEAP) [7] aims to support mutual authentication between a mobile terminal and the AP, thereby defeating man-in-the-middle attacks.

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. Data Encryption Standard (DES) in Cipher Block Chaining (CBC) mode and Advanced Encryption Standard (AES) in Counter with CBC-MAC (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.

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.

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.

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 user'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 signalling 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.

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 has proposed different security architectures for 4G networks, that include: Y-Comm security models for heterogeneous networks, Handover Keying working group (Hokey WG), and ITU X.805 framework.

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 Fig. 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.

*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 and it involves a series of steps.

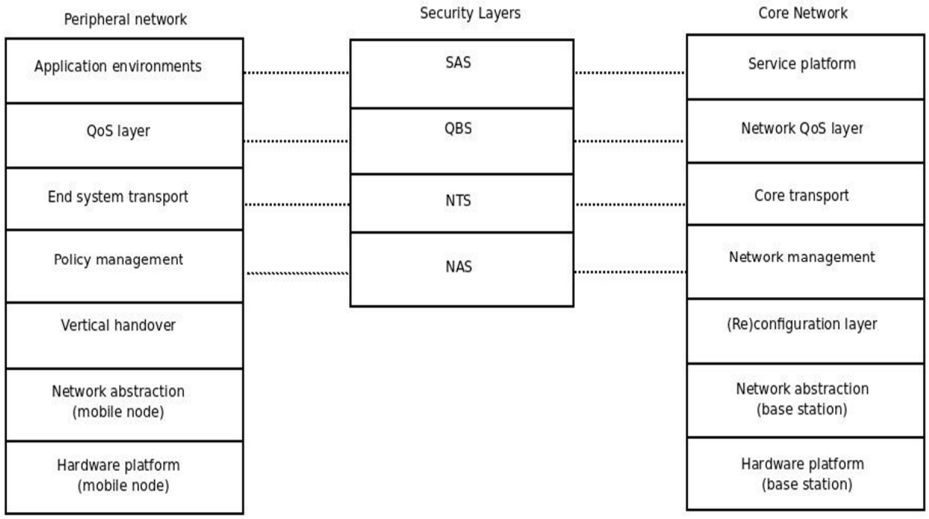

Fig.1: Y-Comm Architecture

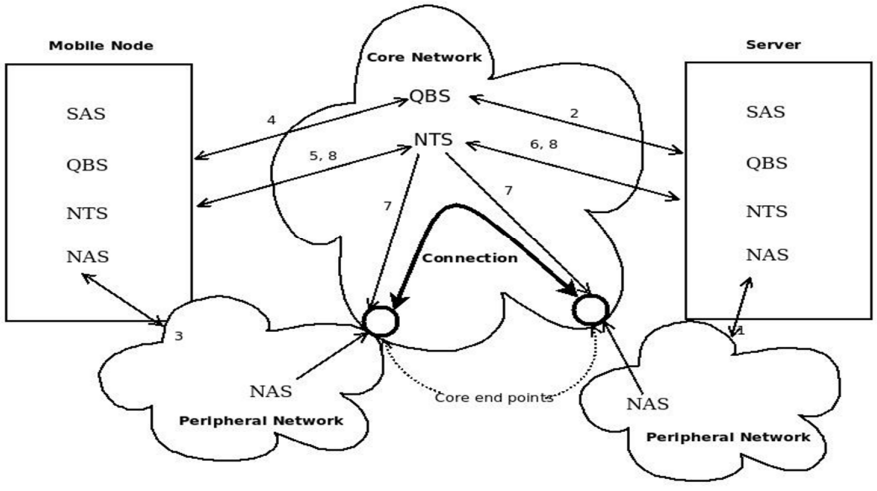

Fig. 2: Connection Security Model

Step 1: The server is started. The NAS module in the server communicates with the NAS module on the Local LAN to get access to its wireless infrastructure.

Step 2: The QBS security module on the server informs the QBS module in the core network about its Service Level Agreement which contains the QoS associated with a connection to this service.
Step 3: The mobile node is started. The NAS module in the mobile node contacts the NAS module in the peripheral networks to gain access to the wireless infrastructure.

Step 4: When the mobile node wants to use the service, the QBS Module in the mobile node contacts the QBS module in the core network and asks for a connection with a given quality of service to be made to the Server. The QBS module returns two core endpoints which must be used to set up the connection.

Step 5: The NTS module on the mobile node contacts the NTS module in the core network and says that it would like a connection to the server, using the core endpoints, the QoS and security parameters.

Step 6: The NTS module in the core network contacts the NTS module on the server to signal an incoming call. At this point, the server can also check the security of the client as well as the security of the connection.

Step 7: If the server accepts the request, then the NTS module in the core network joins the two core endpoints.

Step 8: It then signals to both the client and server that a connection has been established.

Ring-based Security Model: The Ring-Based concept does not allow servers to be directly accessible over the Internet without initially interacting with the network infrastructure. This is done by using the concept of scope where a server acts only within a given scope. See Fig. 3
There are 3 scopes:

Local: Only processes on the same machine are allowed to use a local server. This is achieved by the SAS layer on the local machine.

LAN: Only processes on the same network are allowed to access these servers. This is achieved by the NAS layer of the Peripheral Network.

Global: Global Servers are accessible from any point through the Core Network using Global Services. This is achieved by Core NTS and QBS layers.

Vertical Handover Security Model: In addition to the Authentication, Authorization, Auditing and Cost (AAAC) servers, new entities are involved in the Vertical Handover Security Model (VHSM); the QoS Brokers (QoSB) which monitor the network performance and QoS-related issues (Shown in Fig. 4)

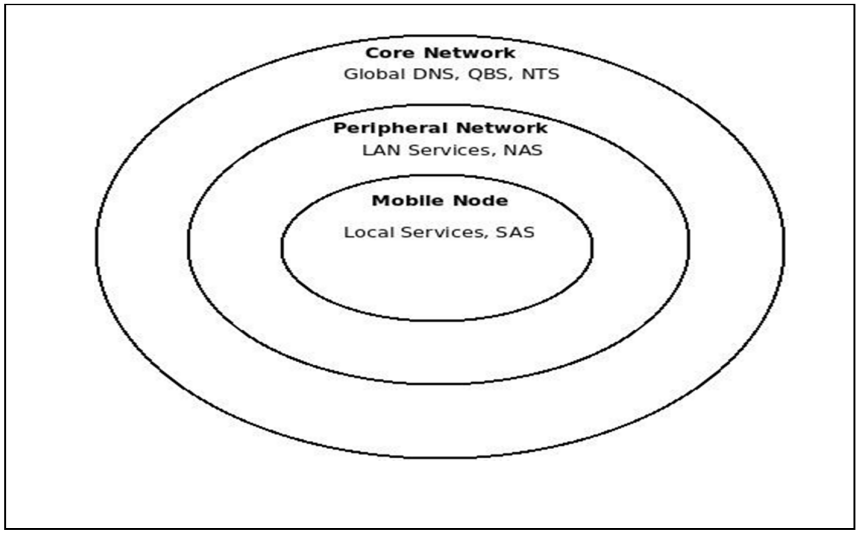

Fig. 3 Ring-based Security Model

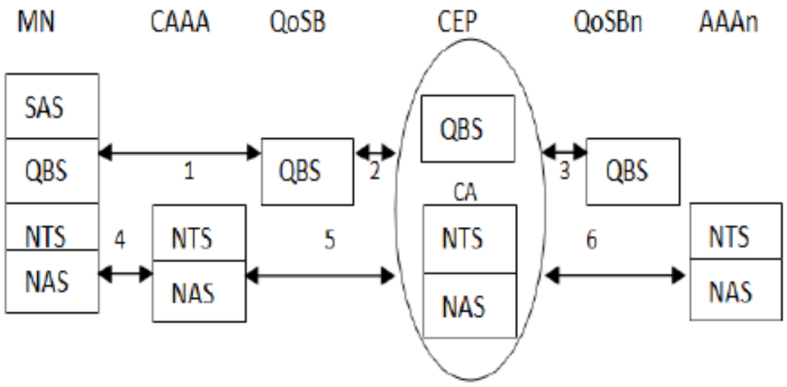

Fig. 4 Vertical Handover Security Model

This model is given by the steps below:
Step 1: The QBS layer of the MN asks the QBS of the QoSB about potential target network for handover with required QoS and security level.

Step 2: The request is passed to the QBS layer of the Core endpoint.

Step 3: If this information has not been already in the Core-End point, the QoS Brokers of all the available networks are probed by the core endpoint.
At the end of this first stage, the MN has a clear idea of the QoS and security suits available at all potential networks in the vicinity and could decide on the target network for future handover.

Step 4: The NAS layer of the MN initiates a Reauthentication process to lunch the security mechanisms in the target network.

Step 5: Through its NAS layer, the currently serving AAA server (CAAA) forwards the reauthentication request along with core information that are used to derive a fresh set of the security parameters for the new network to the NAS layer of a Central Authority (CA) in the Core endpoint.

The MN will check whether it has the same security parameters the AAA of the target network has generated using core information. In case of a match this means that the new network is authentic. Moreover, we presume a certain trust relations between the AAA servers, different trust relationship models might be implemented such as parent-child model where the top level Authority in the Core endpoint issues certificates for all the AAAC servers working in its zone. Alternatively, current Authentication and Key Agreement protocols such as EAP as defined in RFC 5247, might be used to set up a lower-layer secure association among AAA servers.

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 Hockey 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.

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 5, 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.

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.

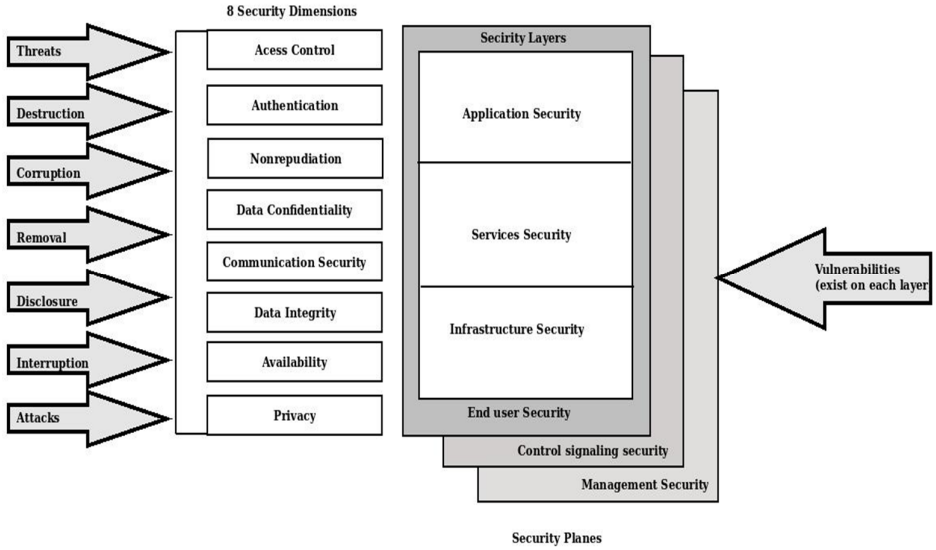

Fig. 5 ITU X.805 Security Model

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.

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.

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, Wi-Fi, 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 Wi-Fi, WiMax, 3G LTE networks and 4G security threats including DoS attack.

Our study on 4G network security architecture shows that, 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.

Security development has no ending, new threats and attacks will arise low-cost and user-managed base station devices will face much more security. 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.

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.