A Survey of Security Threats on 4G Networks

Yongsuk Park, *Member, IEEE*, and Taejoon Park, *Member, IEEE*

***Abstract*—Many communication societies such as ITU and IEEE are working on 4th generation (4G) communication. This paper provides an overview of standardization activities focusing on the network security architectures and a survey of security threats on 4G networks. Our survey shows that a number of new security threats to cause unexpected service interruption and disclosure of information will be possible in 4G due mainly to the fact that 4G is an IP-based, heterogeneous network. We also found there still remain several open issues although many are working on fixing and/or designing new security architectures for 4G.**

***Index Terms*—network security, security architecture, 4G, WiMAX, 3GPP, NGN, NGMN**

I. Introduction

As the 3rd Generation (3G) communication is moving to the 4th Generation (4G) communication, many of societies are preparing themselves for 4G: IEEE 802.16m is working on adapting IEEE 802.16 to IMT (International Mobile Telecommunications)-Advanced (also known as systems beyond IMT-2000), ITU (International Telecommunication Union), that is working on Next Generation Network (NGN) shall discuss IMT-Advanced frequency bandwidth in October, 2007, and WiMAX (**W**orldwide **I**nteroperability for **M**icrowave **Acc**ess) is making a broadband wireless systems based on IEEE 802.16. Also a number of Telecommunication companies such as Vodafone and China Mobile Communications and venders such as Motorola and Samsung gathered and organized NGMN (Next Generation Mobile Networks) to have cost-effective solutions for 4G, and Sprint Nextel is deploying Mobile WiMAX in US and Canada.

Yet many definitions of 4G are available, it shall provide a bandwidth of 100Mb/s in mobile and 1Gb/s in nomadic and it is all-IP with heterogeneous networks where multiple RATs (Radio Access Technology) or RANs (Radio Access Network) interoperate. Some of basic enabling technologies for 4G are OFDM (Orthogonal Frequency-Division Multiplexing) [17], OFDMA (Orthogonal Frequency-Division Multiple Access), [18], and vertical handover protocols. Also, some advanced may include MIMO (Multiple-Input and Multiple-Output) [19], reconfigurable systems and cognitive radio/network [20]. 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 interfaces and end-user devices use open H/W and S/W 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 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. Accordingly, the need for secure networks and services will continue to grow as security will soon become a key differentiator for them.

This paper presents a comprehensive survey of possible security threats on 4G networks. The main contributions of this paper are:

- to oversee the historical evolution of network and security architecture for 4G systems, and
- to pinpoint the possible weaknesses of the current security systems including those of WiFi, WiMAX, 3GPP (3rd Generation Partnership Project) [14] and NGN.

The rest of this paper is organized as follows. Section II presents 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 [10], while the threat analysis for 4G systems is given in Section V. Finally, this paper concludes with Section VI.

II. Network Architecture

A. 4G network

The 4G network as in Fig. 1 [11] is a convergence of multiple heterogeneous access networks such as WiMAX and 3G. Although service subscriber is using any of multiple access networks, it provides services from the same service unit, for example, IP Multimedia Subsystems (IMS). The core

Authors are with the Communication and Networking Lab, Samsung Advanced Institute of Technology, Korea (phone: +82-31-280-9623; fax: +82-31-280-9569; e-mail: {victorious.park, joy.park}@ samsung.com).

network is an all-IP network (IPv6 expected), where a number of its gateways make connections to different access networks as well as service units. Also, QoS-related protocols shall be in place especially for seamless horizontal and vertical handover. Moreover, because a region may be covered by multiple RANs, selecting an appropriate RAN becomes an important issue.

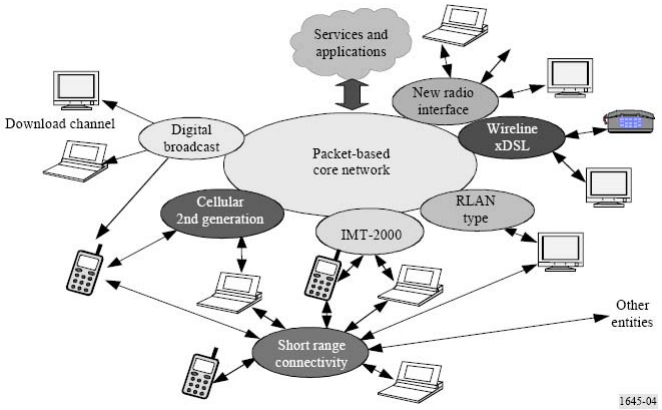

Fig. 1. IMT-advanced 4G network system specified in ITU

B. WiMAX Architecture

The Network Reference Model (NRM) for WiMAX architecture is shown in Fig. 2 [12]. It has an access serving network to provide service stations or mobile stations a connection to Network Service Provider.

Three access network profiles are considered by WiMAX. Profile A has Base Transceiver Station (BTS) and Base Station Controller (BSC) separated. Functions like AAA, paging, routing are in the BSC so, ciphering happens in BS. In profile B, most functions including AAA and paging reside in BS. In profile C, AAA, paging, routing are in ASN-GW (AcceSs Network-GateWay).

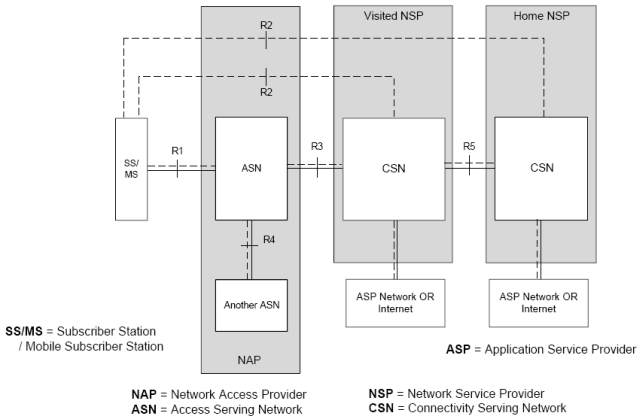

Fig. 2. Network Reference Model (NRM) of WiMAX

C. 3GPP LTE Architecture

3GPP LTE architecture has two core networks [13]: GPRS core network to offer network connections for existing RANs (for example, GERAN and UTRAN) and Evolved Packet Core network to give network connections to Evolved RAN and non-3GPP IP access. IP service for example IMS is provided via Evolved Packet Core to any RANs; it is connected to SAE (System Architecture Evolution) Anchor point, which has a connection to GERAN/UTRAN via SGSN.

In 3GPP access network radio resource control function is in eNB (e-Node B) while AAA function and ciphering functions are in aGW (access-GateWay).

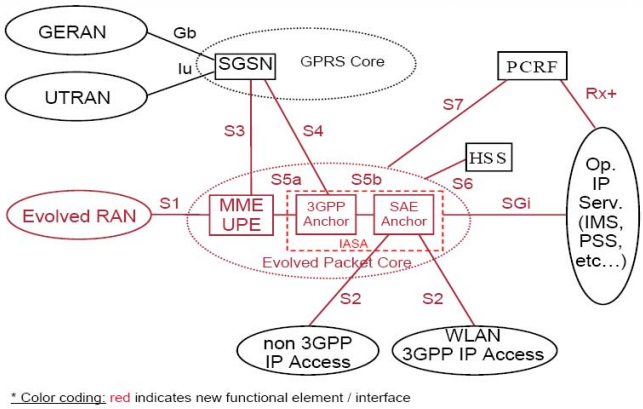

Fig. 3. Network Architecture of 3GPP LTE

D. ITU Architecture for Ubiquitous Coverage

A region (macro, micro, pico cells or hot spot) may be covered by one access network and, on the other hand, more than one access networks may cover the same region. Taking the later, ITU describes network architecture to calculate frequency bandwidth allocation of multiple RANs and to have its ubiquitous coverage [9]. At first, it classifies multiple RANs into four groups. RAT Group 1 includes pre-IMT systems, IMT-2000 and its enhancement; Group 2 includes systems beyond IMT-2000; Group 3 includes existing radio LANs and their enhancements; Group 4 includes Digital Mobile broadcasting Systems and their enhancements. RAT Group 1 supports 1 to 2.5 Mb/s data rate for macro, micro, pico cells. RAT Group 2 supports 50 to 1000 Mb/s data rate for all cells. RAT Group 3 supports 50 to 100 Mb/s for pico cell and hot spot.

Depending on tele-density (or traffic volume) of the region, cell sizes may be different. Macro cell radius is more than 1 km in urban, in that tele-density is expected to be high, more than 40 km in rural, in that that is expected to be low. Micro cell radius is from 50 m to 1 km while pico cell radius is less than 50 m and hot spot is several tens of meters. Having this ubiquitous coverage architecture, NGN's network architecture is similar to that of 3GPP.

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 integrated into both the network core and the end-user devices. The key objectives in designing the security architecture can be summarized as:

- *availability* that enforces networks and services not to be disrupted or interrupted by, for example, malicious attacks;
- *interoperability* that ensures the security solutions can avoid interoperability problems, e.g., by using generic solutions applicable to most of the NGN applications and service scenarios;
- *usability* that makes it easy for the end-users to use the security-enabled services;
- *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 [10], [1] 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 [16]. 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 IMS security relies 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 [16].

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

[1] See Section IV for details of X.805 specification.

Access Sub-System (NASS) strongly depends on the access technology. The access view security uses IPsec transport mode and Authentication and Key Agreement (AKA) on top of the ISIM application on UICC in the end-user device.

A unique requirement of NGN is its support for more business roles ranging from regional network operators to service providers. Hence, many of the external connectivity points will likely be inter-operator interfaces, which may become potential sources of vulnerabilities. To protect these interfaces, NGN specifies Security Gateways (SEGs) that enforce security policy between domains.

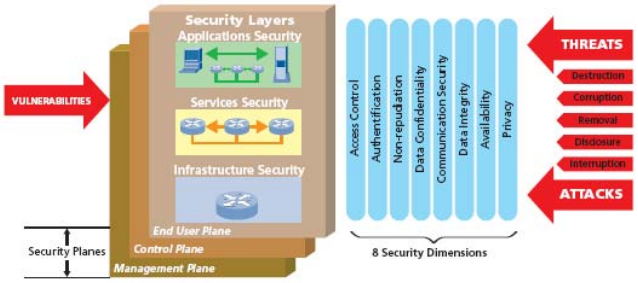

Fig. 4. X.805 Network Security Analysis

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 systems may happen in any layers such as services and infrastructure 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 [3] [10]. 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 threats [10].

In X.805, the network security is, as shown in Fig 4, 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 and/or attacks of destruction, corruption, removal, disclosure, 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, for instance, WiMAX access service that end-users receive from networks, 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. 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 objectives 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.

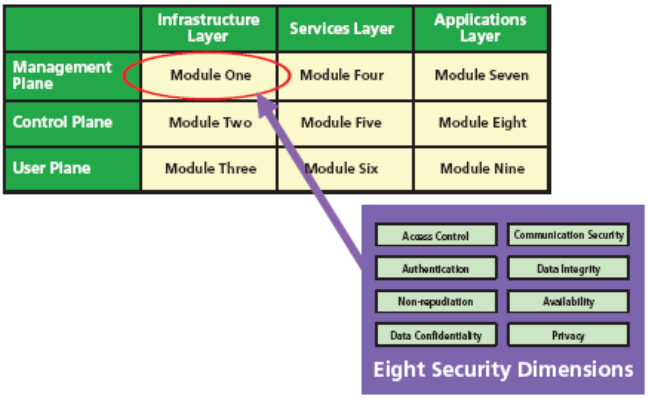

Fig. 5. X.805 Modular Approach

V. Security Threats

To manage the threats the network infrastructure is exposed to, it is essential to clearly identify the key risks and threats, e.g. using the methodology of Section IV, to develop and/or refine security protocols. In this section, we present a case study of security analyses for well-known standards: Wi-Fi, WiMAX, 3GPP and ITU NGN.

A. Wi-Fi Security

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 cafes, airports, hotels and shopping malls where security is seemingly less critical, although the cost benefits of Wi-Fi could be attractive to enterprise environments thanks to increased mobility, lower deployment/operational costs, and flexibility. Accordingly, security researchers have focused on security threats and solutions in Wi-Fi networks [1] [2] to make it applicable to the enterprise environments.

As shown in [1], 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. Regarding this, a comprehensive security evaluation based on the ITU-T X.805 standard (in Section IV) has been performed by Bell Labs [3].

To remedy the security flaws of Wi-Fi, several solutions have been proposed in [1][4][5][6]. The Robust Security Network (RSN) for the IEEE 802.1x standard's port based network access control [4] is a layer-2 authentication mechanism and specifies how EAP can be encapsulated in the Ethernet frames. LEAP [5] aims to support mutual authentication between a mobile terminal and the AP, thereby defeating man-in-the-middle attacks. RSA Laboratory and Cisco have developed TKIP [6] to mitigate the weakness of RC4 via frequent renewal of encryption key. Authors of [1] proposed an automated mechanism to refresh the encryption key seamlessly.

To summarize, the Wi-Fi security has made significant improvement in the last few years by taking a systematic approach of discovering security weaknesses and developing appropriate countermeasure. Hence, by using the state-of-the-art security protocols and mechanisms, a reasonably secure Wi-Fi network can be deployed with reasonable tolerance to risks in most enterprise environments. The study of Wi-Fi security tells us that other networking environments will undergo similar steps until achieving an acceptable level of security.

B. WiMAX Security

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 for fixed and mobile architectures, respectively. These two standards specify different sets of security mechanisms.

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, with an option to use a proprietary encryption algorithm.

However, a number of weaknesses were discovered in IEEE 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, equally contributing to the values of keys. Third, it does not support integrity protection of management frames, exhibiting a potential risk of denial-of-service (DoS) attacks. Finally, it does not define how to manage, store, renew and revoke certificates.

In IEEE 802.16e-2005, an improved version of PKM is developed to fix known vulnerabilities of PKM as well as offer more options. The key difference is that the improved PKM makes it mandatory to perform mutual authentication between MS and BS via RSA and/or EAP (Extensible Authentication Protocol). Besides, most of the management frames are now signed to ensure integrity protection, and AES-based encryption (in CBC, CTR and CCM modes) is used to provide communication flow protection.

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. It is, therefore, important for the researchers and standards developers to keep on improving the security protocols as well as uncovering possible unknown vulnerabilities, similarly to the case of Wi-Fi.

C. 3GPP LTE Security

Security in cellular systems evolved as the generation changes. In the first generation (1G) cellular system, there was not much consideration for security; because there was no over-the-air encryption in place and mobile phones could be easily cloned by intercepting the serial number, eavesdropping of conversation could easily happen.

The 2G, exemplified by Global System for Mobile (GSM), uses Authentication and Key Agreement (AKA), called GSM AKA, for encryption and authentication. It uses a challenge-response mechanism, where the user proves its identity by providing a response to a time-variant challenge raised by the network. However, its security is weak in that its authentication is only unidirectional; the user cannot authenticate the serving network. Also, authentication data (which are called triplets) can be reused indefinitely and the authentication information and cipher keys can be reused.

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. In addition, a sequence number is used for freshness where two counters–each for network and mobile terminal–are synchronized for sequence number verification [14] [15].

Although the 3GPP AKA has been accepted as reliable and used, there still exist weaknesses in 3GPP AKA as shown in [7]. The weaknesses include (1) redirecting user traffic using false BS and mobile terminals, (2) given the fact that the counter value of set to a high value by adversary, the mobile terminal's life time may be shortened, (3) because a home

network keeps a counter and dynamically synchronized for every mobile terminal, a fault in counter database may affect all mobile terminals. Also because resynchronization is requested by MT, this may result in resynchronization message attack to the home network.

D. Possible 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 include: (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. Conclusions

To better understand the security of 4G networks, we studied the standardization activities of chosen international communication societies (IEEE, WiMAX, 3GPP, and ITU) with an emphasis on network security issues. We first summarized their network and security architectures and then made comprehensive threat analyses to characterize the known (or possible) risks to each of them. Our threat analyses indicated (1) that 4G will inherit all the security problems of underlying access networks (such as 2/3G cellular networks, WiMAX networks, sensor networks and so on) because of their heterogeneous and open architecture, and (2) 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.

Security development has no ending; new threats and attacks shall rise as the standards and technologies get realized. For example, it is expected that pico or even femto base stations will become popular in 4G, but such low-cost and user-managed base station devices will face much more security attacks due in part to their high accessibility. Hence, the comprehensive threat analysis of, and the development of appropriate countermeasure for, the entire 4G systems must be made in parallel with the evolution of 4G architecture, which are our on-going research.

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] Cisco, "Lightweight Extensible Authentication Protocol (LEAP)," avail. from http://www.cisco.com/warp/public/102/wlan/nextgen.html.

[6] R. Housley and D. Whiting, "Alternate Temporal Key Hash," *IEEE P802.11 Wireless LANs,* April 2002.

[7] 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.

[8] ITU-R M.2074, "Radio aspects for the terrestrial component of IMT-2000 and systems beyond IMT-2000," 2005.

[9] WiMAX Forum Network Architecture, "Stage 2: Architecture Tenets, Reference Model and Reference Points," 2007.

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

[11] ITU-R M.1645, "Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000," 2003.

[12] WiMAX Forum Network Architecture (Stage 3: Detailed Protocols and Procedures), 2007.

[13] 3rd Generation Partnership Project; Technical Specification Group SA; 3G Security, "Security Architecture, version 4.2.0, Release 4," 3GPP, TS 3.102, 2001.

[14] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security, "Formal analysis of the 3G authentication protocol, version 3.1.0," 3GPP, TR 33.902, 1999.

[15] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects;3GPP System Architecture Evolution: Report on Technical Options and Conclusions, TR 23.882, 2007.

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

[17] E. F. Casas and C. Leung, "OFDM for data communication over mobile radio FM channels—part I: Analysis and experimental results," *IEEE Trans. Commun.*, vol. 39, pp. 783–793, May 1991.

[18] Jo Woon Chong, Bang 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.

[19] 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 – 1518, April 2006.

[20] 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 Communications Magazine*, Volume 44, Issue 12, pp. 51 - 57, Dec. 2006.