Wireless LAN Security Solutions for Secure Wireless Communications

Su-Yong Kim, Duck-Ki Ahn, Jae-Sung Roh, Chang-Heon Oh and **Sung-Joon Cho**, *Member, KIMICS*

Abstract—The 4th generation mobile communications, through several radio access networks such as WLAN, Bluetooth, UMTS, GPRS, CDMA 1X, and IMT-2000 in the same area offering different type of coverage, will support interactive multimedia services in additions to wider bandwidths, higher bit rates, and service portability. Regardless of various radio access networks, they will also support robust security mechanisms, as well as seamless mobility and common authentication. In this paper, we give an overview of WLAN security and examine its security problems. We also explain the enhanced security schemes, such as port-based authentication, EAP, and IEEE 802.1X. For secure wireless communications, several possible security solutions are offered and evaluated in various respects to improve WLAN security. This paper will make a contribution to provide more secure wireless communications to cellular operators embracing WLAN technology as a means to generate new revenues based on data services.

Index Terms—Wireless LAN security solutions, WLAN-Cellular, 802.1X and EAP, VPNs and IPSec

I. INTRODUCTION

As one of the next generation mobile communications, the requirements of 4th generation mobile communications can be described as providing various services, such as high-speed data services and IP-based access to Radio Access Network (RAN), etc. The exact specifications for the 4th generation have not yet been specified, but the recent trend [1,2] is that various interface techniques, such as WLAN, Bluetooth, UMTS, GPRS, CDMA 1X, and IMT-2000, are integrated in IP-based networks as an overlay structure [3]. For example, Fig. 1 shows a WLAN-Cellular overlay network.

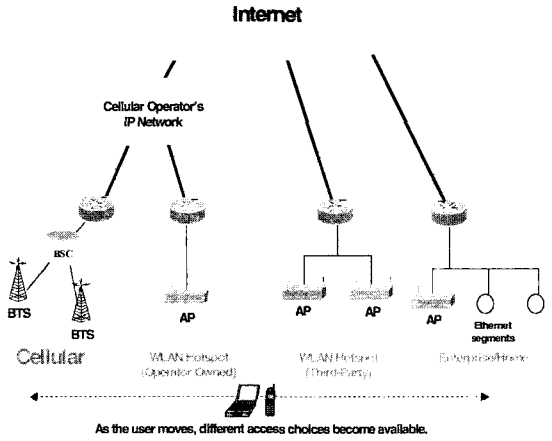


Fig. 1 WLAN-Cellular Overlay Network

Wireless LANs are becoming more ubiquitous, especially in the consumer markets. Home WLAN devices are inexpensive and easy to configure, eliminating the need for ethernet wiring in the home. Commercial enterprises, such as hotels, coffee shops, bookstores, and even some fast food restaurants provide wireless access. When providing network services to users in older buildings, network managers are finding it cost effective to use WLANs rather than new fiber and ethernet cabling. They are also finding that the use of WLANs enables them to set up network connectivity quickly and efficiently. Students can access the campus network from points located throughout the campus. These WLAN standards are specified in the IEEE 802.11 documents [4,5,6,7]. Various subgroups of the 802.11 standard exist, addressing various frequency bands and data speeds.

Of these, the 802.11i task group is focusing on the vulnerabilities of the current encryption mechanisms. This 802.11i standard [8] is not yet complete, however, preliminary disclosures indicate that the new standard will use the Advanced Encryption Standard (AES) as the encryption method. AES is a more robust encryption mechanism as compared to the RC4 algorithm currently in use. In addition, the Message Integrity Code (MIC) is to be included in the standard, instead of a vendor-specific feature. The current 802.1X [9] operation is to be incorporated into the 802.11i standard as well.

Manuscript received September 10, 2003.

S. Y. Kim is with the Dept. of Inform. & Telecomm. Eng., Graduate School of Hankuk Aviation Univ., Koyang-Si, Kyounggi-Do, 412-791, Korea (Tel : +82-2-3158-1518, Fax : +82-2-3158-1935, E-mail : sykim@mail.hangkong.ac.kr)

D. K. Ahn is with the Dept. of Inform. & Telecomm. Eng., Graduate School of Hankuk Aviation Univ., Koyang-Si, Kyounggi-Do, 412-791, Korea (Tel : +82-2-3158-1518, Fax : +82-2-3158-1935, E-mail : palangsea@mail.hangkong.ac.kr)

J. S. Roh is with the Dept. of Inform. & Comm. Eng., Seoil College, Myunmok-8 Dong, Jungrang-Gu, Seoul, Korea (Tel : +82-2-490-7206, Fax : +82-2-490-7407, E-mail : jsroh@seoil.ac.kr)

C. H. Oh is with the School of Information and Technology, Korea University of Technology and Education, P.O. Box 55, Cheonan, 330-600, Korea (Tel : +82-41-560-1187, Fax : +82-41-564-3261, E-mail : choh@kut.ac.kr)

S. J. Cho is with the School of Electronics, Telecomm. and Computer Eng., Hankuk Aviation Univ., Koyang-Si, Kyounggi-Do, 412-791, Korea (Tel : +82-2-3158-1518, Fax : +82-2-3158-1935, E-mail : sjcho@mail.hangkong.ac.kr)

The rest of this paper is organized in the following manner. In the next section, we will give an overview of WLAN security and examine its security problems. In section three, we will explain the enhanced security schemes, such as port-based authentication, Extensible Authentication Protocol (EAP), and IEEE 802.1X. In section four, several possible security solutions will be offered and evaluated in various respects to improve WLAN security. In section five, we will present conclusions.

II. OVERVIEW OF WLAN SECURITY

IEEE 802.11 [4] was ratified in 1999. This standard governs the physical (PHY) and Medium Access Control (MAC) layers for the realization of WLANs. Variations on the PHY have been introduced in later supplements [5,6,7] to extend the data rate capabilities up to 54 Mbps. Although improvements have been made on the PHY, the MAC, which governs WLAN security capabilities, has remained the same.

A. Authentication

There are two types of authentication methods defined in 802.11 MAC layer. These are Open System Authentication and Shared Key Authentication. In Open System Authentication, a simple two-step process is followed to authenticate a mobile station. It is essentially a null authentication algorithm that, when activated on the authenticator, will successfully authenticate any other mobile station that requests Open System Authentication.

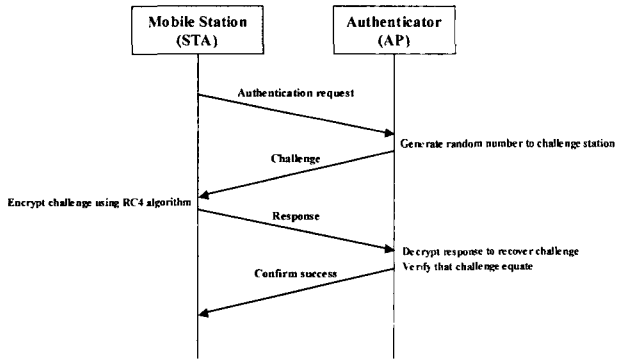


Fig. 2 Shared Key Authentication Procedure

Like Fig. 2, Shared Key Authentication supports a challenge-response mechanism for authenticating a mobile station. In this method, a secret key is shared between the authenticator and the mobile station being authenticated. The mobile station sends an authentication request to the authenticator (Step 1). The authenticator generates a random challenge and passes the challenge to the mobile station (Step2). The mobile station generates a response to the challenge by passing the challenge text through the 802.11 WEP encryption algorithm (Step 3). The authenticator decrypts the WEP-encrypted authentication frame and compares the decrypted challenge text with the original challenge sent to the mobile station. If the values are the same, the authenticator replies success (Step 4).

B. Privacy

The IEEE 802.11 standard stipulates an optional scheme called Wired Equivalent Privacy (WEP), which offers a mechanism for secure WLAN data streams. WEP uses a symmetric scheme where the same key and algorithm are used for both encryption and decryption data. WEP uses the combination of a secret key and Initialization Vector (IV) as a seed for a Pseudo Random Number Generator (PRNG), which generates the encryption key sequence on a packet basis. This encryption key sequence is then XORed with the plaintext of the message to arrive at the ciphertext. Then, the ciphertext is transmitted over the air in combination with the IV used to generate the encryption key for this packet. Fig. 3 shows the WEP encryption and decryption block diagram.

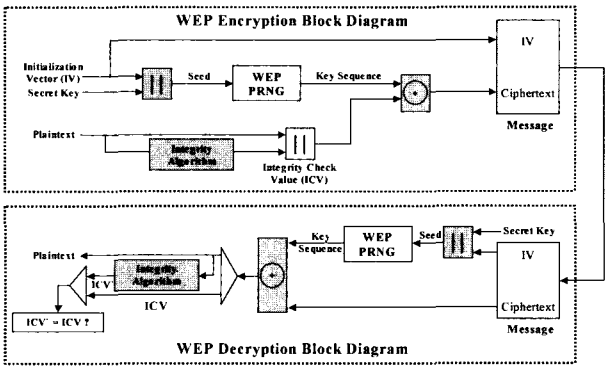


Fig. 3 WEP Privacy Block Diagram

On receiving WEP-encrypted packet, the station deciphers the encryption using the combination of the same secret key and the IV sent in the plaintext of the message. This provides the same key sequence that was used to encrypt the packet. The key sequence is then XORed with the ciphertext of the packet to arrive at the plaintext. To validate the plaintext, the Integrity Check Value (ICV') is recalculated on the plaintext and compared with the ICV contained in the message. If both agree, the decryption is successful.

C. Security Problems

802.11 systems are vulnerable to both passive and active attacks due largely to WEP particular implementation of RC4 stream ciphering, and also vulnerable to keystream reuse. The keystream is generated from both the secret key and IV used in the encryption. A well-known issue with stream ciphers is that encrypting two messages with the same RC4 seed can reveal information about both messages. WEP RC4 seed consists of both the secret key and IV. 802.11 does not provide a dynamic key distribution mechanism to maintain key freshness, and many 802.11 implementations use the global and static key provisioning. Therefore, the IV provides the only uniqueness in seeds between messages. The issue with this is two-fold. First, the IV field is only 24 bits in length, causing a high probability of IV reuse. Second, particular implementations of IV generation algorithms are quite predictable, increasing the IV reuse probability. This problem is compounded when all users of a network use the same and static WEP key. Once one user's traffic has been

compromised, all traffics become compromised and the network is no longer secure.

Another issue of 802.11 security is its lack of network authentication. During authentication procedures, the AP authenticates the mobile station using either Open System Authentication or Shared Key Authentication. There is no parallel authentication of the network to the user offered by 802.11. This can lead to additional man-in-the-middle attacks.

III. ENHANCED SECURITY SCHEMES

IEEE 802.1X [9] provides port-based authentication in WLAN access networks. It is included as a requirement for WLAN authentication in the IEEE 802.11i draft standard as a portion of the enhancements that will shore up 802.11 security products in the future. Although IEEE 802.1X does not solve all the problems associated with WEP implementation of RC4 stream ciphering, it does provide an incremental step in the right direction. IEEE 802.1X provides the improvements on IEEE 802.11 security, such as mutual authentication and dynamic key management.

A. Port-based Authentication

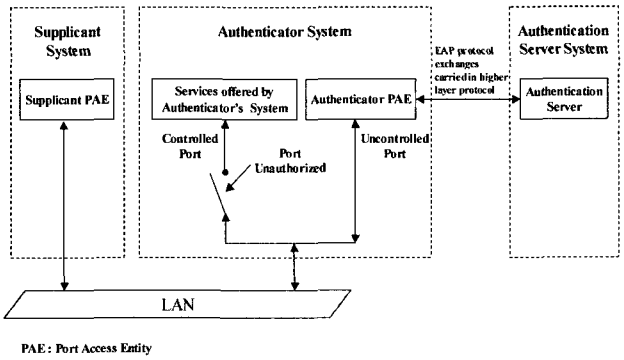


Fig. 4 IEEE 802.1X Port-based Authentication

IEEE 802.1X defines a method for authentication within the context of IEEE 802 networks. This method, called port-based Access Control (AC), consists of interaction among three entities that must be present in the network. These are the Supplicant, the Authenticator, and the Authentication Server.

The Authenticator logically consists of a controlled port and an uncontrolled port for each Supplicant in the system. Prior to successful authentication, the two logical ports are as shown in the Authenticator System of Fig. 4. The controlled port allows the exchange of PDUs between systems on the LAN only when the current state of the port is authorized. The uncontrolled port allows the exchange of PDUs regardless of authorization state. In addition, the uncontrolled port is used strictly for authentication message between the Supplicant and Authenticator. Once a successful authentication has been resulted between the Supplicant and the Authentication Server, the controlled port will transit to an authorized state and all traffics will be passed through this port.

B. EAP Framework

EAP [10] is a flexible protocol in its extensibility, allowing for large variation in authentication methodology to be applied to the same message framework provided by EAP. This framework includes a simple Request/ Response packet format. Once the authentication has completed, the EAP framework is used to indicate Success or Failure of the authentication attempt. The actual authentication logic is handled by the EAP methods that are indicated by the type field in the EAP message header. These methods can be viewed as a plug-in to the EAP layer. This aspect of EAP authentication methods is captured in the EAP architecture diagram shown in Fig. 5.

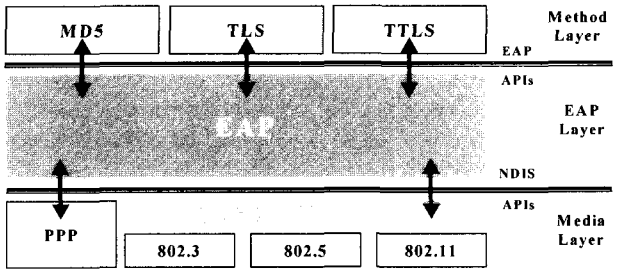


Fig. 5 EAP Architecture Diagram

As can be seen in Fig. 5, EAP methods can be added on top of the framework provided by EAP and then applied to multiple access networks over both PPP and 802.1X. This becomes quite useful in hybrid IP networks, where many options exist for connecting a device to the network. In such a situation, the same authentication methods may be applied, regardless of how the user chooses to connect to the network.

C. Benefits of IEEE 802.1X

By providing the framework for EAP authentication methods to be applied to WLAN access networks, and using port-based authentication to control access to the network, 802.1X opens the door for improvements to the built-in security of IEEE 802.11 networks. Depending on the EAP methods, such things as mutual authentication, dynamic key management, and certificate-based authentication are possible in WLAN access networks with no modifications required in the WLAN equipments. The particular EAP methods are implemented only at the endpoints, allowing for a kind of plug-and-play approach to add new authentication methods. These new capabilities have provided the opportunities to the cellular operator to extend its proven cellular security technology into the WLAN environment.

IV. POSSIBLE SECURITY SOLUTIONS

There are several approaches to WLAN security against a specific threat or several attack methods. Security can be enhanced to some degree simply by the use of proper security policies, equipment configuration, and system design. For example, proper security policies should limit the access of individual users to specific applications and servers.

The modest level of WLAN security can be obtained by proper AP configuration practices. First, default configurations should be changed as applicable to the network operation. The SSID and shared WEP keys should be changed from their default state. The SSID used should be unique to the system. WEP keys should be based on a random hexadecimal number ranging from 0-F and set for 128-bit mode. This protects against hackers guessing the SSID or WEP keys based on typical vendor default configurations.

The maximum level of WLAN security can be available in the AP. This may include the use of Temporal Key Integrity Protocol (TKIP) and a MIC. TKIP helps to protect against attacks via the most vulnerable segment of the WEP key, which is the Initialization Vector (IV). TKIP provides a per-packet key to mitigate this threat. To help ensure the integrity of the transmitted data, the MIC is used to protect against data manipulation by the hacker. Any changes to the message will affect the MIC value, which is based on a seed value, the source and destination MAC addresses, and the message payload. An improper MIC value will cause the packet to be discarded.

An elevated level of security involves enhanced encryption and unit authentication. This may include several mechanisms, such as 802.1X and EAP, VPNs and IPSec. These methods will be considered as potential security solutions.

802.1X and EAP solution is based on dynamic WEP keys and mutual authentication. The 802.1X standard describes how EAP information is transferred over the WLAN. There are several adaptations of EAP, some of which are proprietary to specific vendors like EAP Message Digest 5 (EAP-MD5), EAP Transport Level Security (EAP-TLS), EAP Tunneled Transport Level Security (EAP-TTLS), etc. These forms use a transport layer tunnel to complete the EAP authentication process. EAP operates using a unique key for each user and each session. Unique WEP keys coupled with a user log-on mitigate vulnerabilities due to stolen or lost client cards or devices. The use of mutual authentication also provides protection against rogue APs and man-in-the-middle attacks.

Table 1 EAP Authentication Methods

EAP Method	EAP-MD5	EAP-TLS	EAP-TTLS
Requirement	Mandatory	Optional	Optional
Authentication Credentials	Password Only	Client-Certificate Server-Certificate	Client-Password Server-Certificate
Authentication Server	Standard MD5	Certificates Infrastructure Required	ServerCertificates Standard PAP, CHAP MSCHAP User Database
Mutual Authentication	Not Supported (Client Only)	Supported	Supported
Key Generation	No	Dynamic KEY	Dynamic KEY
Client Support	Microsoft, Funk, Meetinghouse	Microsoft, Funk, Meetinghouse, Cisco	Funk, Meetinghouse

EAP authentication methods can be implemented without any changes to the AP or the Network Interface Card (NIC) firmware. We compare EAP authentication methods in Table 1.

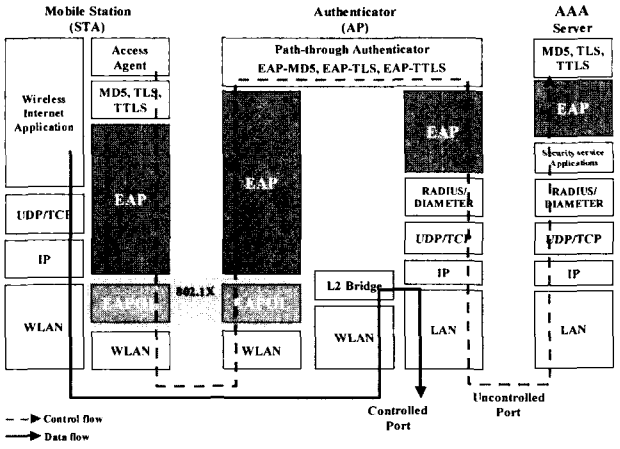


Fig. 6 EAP and 802.1X Authentication Protocol Stack

The EAP and 802.1X authentication protocol stack is illustrated in Fig. 6 Using two-way authentication, a mobile station that associates with an AP cannot gain access to the network until network logon credentials are verified. The client and AAA server perform a mutual authentication, with the client authenticated by the supplied username and password, or a certificate. The client and AAA server then derive a client-specific WEP key to be used by the client for the current logon session.

802.1X and EAP solution mitigates the threats due to the vulnerabilities of WEP, the threats from rogue APs, the man-in-the-middle attacks, and the theft of the mobile hardware. In addition, the threats from IP and MAC spoofing are mitigated.

Another method for WLAN security is VPNs and IPSec solution. An IPSec client is placed on all WLAN clients, which requires that a VPN tunnel be set up to enable transport of the client traffic onto the wired network. By using encryption methods such as 3DES, confidentiality of the transferred data can be obtained. The VPN tunnel is terminated at the VPN concentrator, which can also function as an authentication device. In general, however, an authentication server is used. VPN operation requires that the user log on to the network using the VPN client application. VPNs also support the use of one-time passwords.

VPNs and IPSec solution is typically used when the sensitivity of the data is paramount. However, it should be noted that this approach is more costly and complex in comparison to EAP and 802.1X solution. Another factor to consider is the effect on the wired network traffic. The use of VPN can introduce additional overhead and may increase the network traffic in specific areas since all WLAN traffics must be funneled through the VPN concentrator. To use the VPN approach, the network designer must add a VPN concentrator, authentication server and appropriate software to the network infrastructure. Corresponding VPN client software is required for each mobile.

VPNs and IPSec solution, like 802.1X and EAP solution, can mitigate the threats due to the vulnerabilities of WEP, the threats from rogue APs, the man-in-the-middle attacks, and the theft of the mobile hardware. However, the threats from IP and MAC spoofing can't be mitigated until the IPSec tunnel has been set up.

V. CONCLUSION AND FUTURE WORKS

This paper gave an overview of WLAN security and examined its security problems. This paper also explained the enhanced security schemes, such as port-based authentication, EAP, and IEEE 802.1X. For secure wireless communications, several possible security solutions were being offered and evaluated in various respects to improve WLAN security. Potential security solutions described in this paper include 802.1X and EAP solution, VPNs and IPSec solution. It is highly recommended that WLAN designers specify and implement 802.1X and EAP solution using dynamic WEP keys and mutual authentication. 802.1X and EAP solution can provide a cost effective solution as against VPNs and IPSec solution, which is typically used when the confidentiality of the data is of primary importance.

This paper will make a contribution to provide more secure wireless communications to cellular operators embracing WLAN technology as a means to generate new revenues based on data services. The future work will include the integrated security solutions for secure WLAN-Cellular integration.

ACKNOWLEDGMENT

This research was supported by IRC (Internet Information Retrieval Research Center) in Hankuk Aviation University. IRC is a Kyounggi-Province Regional Research Center designated by Korea Science and Engineering Foundation and Ministry of Science & Technology.

REFERENCES

[1] R. Berezdivin, R. Breinig, and R. Topp, "Next-Generation Wireless Communications Concepts and Technologies," *IEEE Communications Magazine*, pp. 108-116, March, 2002.

[2] T. Otsu, I. Okajima, N. Umeda, and Y. Yamao, "Network Architecture for Mobile Communications Systems Beyond IMT-2000," *IEEE Personal Communications*, pp. 31-37, October, 2001.

[3] Hyo Soon Park, Sung Hoon Yoon, Tae Hyoun Kim, Jung Shin Park, Mi Sun Do, and Jai Yong Lee, "Vertical Handoff Procedure and Algorithm between IEEE802.11 WLAN and CDMA Cellular Network," *CIC 2002*, LNCS 2524, pp. 103-112, 2003.

[4] IEEE Std 802.11, "Standard for Local and Metropolitan Area Networks : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," August, 1999.

[5] IEEE Std 802.11a, "Standard for Local and Metropolitan Area Networks : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications : High-speed Physical Layer in the 5 GHZ Band," September, 1999.

[6] IEEE Std 802.11b, "Standard for Local and Metropolitan Area Networks : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications:Higher-Speed Physical Layer Extension in the 2.4 GHz Band," November, 2001.

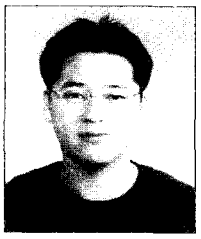
[7] IEEE P802.11g/D8.2, "Draft for Local and Metropolitan Area Networks : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications : Further Higher Data Rate Extension in the 2.4 GHz Band," April, 2003.

[8] IEEE Std 802.11i/D4.1, "Draft Supplement to IEEE Standard for Local and Metropolitan Area Networks: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements," July, 2003.

[9] IEEE Std 802.1X-2001, IEEE Standard for Local and Metropolitan Area Networks: Port-Based Access Control.

[10] IETF RFC 2284, Extensible Authentication Protocol (EAP), March, 1998.

Su-Yong Kim, Member KIMICS
Received the B. S. and M. S. degrees in telecommunication and information engineering from Hankuk Aviation University, Kyounggi-Do, Korea in 1997 and 1999, Respectively. He is currently completing the Ph. D. degree in information and telecommunication engineering at Hankuk Aviation University, Kyounggi-Do, Korea. His research interests are in the areas of wireless security, wireless internet platform and WLAN-Cellular integration. He is a member of Korean Institute of Communication Sciences, a member of Korea Navigation Institute, and a member of Korea Institute of Maritime Information & Communication Sciences.



Duck-Ki Ahn, Member KIMICS
Received the B. S. degree in telecommunication and information engineering from Hankuk Aviation University, Kyounggi-Do, Korea in 2003. He is currently completing the M. S. degree in information and telecommunication engineering at Hankuk Aviation University, Kyounggi-Do, Korea. His research interests are in the areas of wireless security and communication protocol. He is a member of Korean Institute of Communication Sciences, a member of Korea Navigation Institute, and a member of Korea Institute of Maritime Information & Communication Sciences.

Jae-Sung Roh, Member KIMICS
Received the B. S. and M. S. degrees in the telecommunication and information engineering from Hankuk Aviation University, Kyounggi-Do, Korea in 1990 and 1992, Respectively. He received the Ph. D. degree from Hankuk Aviation University, Kyounggi-Do, Korea in 2000. He is currently an assistant professor of the Dept. of Inform. & Comm. Eng., Seoil College, Seoul, Korea. His research interests are in the areas of wireless security and performance evaluation of mobile network. He is a member of Korean Institute of Communication Sciences, a member of Korea Electromagnetic Engineering Society, a member of Korea Navigation Institute, and a member of Korea Institute of Maritime Information & Communication Sciences.

Chang-Heon Oh, Member KIMICS
Received the B. S. (*magna cum laude*) and M.S.E. degrees in telecommunication and information engineering from Hankuk Aviation University, Kyounggi-Do, Korea, in 1988 and 1990, respectively. He received the Ph.D. degree in avionics engineering from Hankuk Aviation University, Kyounggi-Do, Korea, in 1996. From February 1990 to August 1993, he was with Hanjin Electronics Co., where he was involved in the research and development of radio communication systems. From October 1993 to February 1999, he was with the CDMA R&D center of Samsung Electronics Co., where he was involved in the design and development of CDMA cellular systems and CDMA PCS systems for successful commercial CDMA deployment in Korea. Since March 1999, he has been with the Department of Information and Communication Engineering, Korea University of Technology and Education, Chonan, Korea, where he is currently an assistant professor. His research interests are in the areas of communication theory, radio communications, and mobile communication systems design with particular emphasis on CDMA cellular system. He is a member of Korean Institute of Communication Sciences, a member of Korea Electromagnetic Engineering Society, a member of Korea Navigation Institute, and a member of Korea Institute of Maritime Information & Communication Sciences.

Sung-Joon Cho, Member KIMICS
Received the B. S. degree in telecommunication engineering from Hankuk Aviation University, Kyounggi-Do, Korea in 1969, the M. S. degree in the telecommunication engineering from Hanyang University, Seoul, Korea in 1975 and the Ph. D. degree in telecom-munication engineering from Osaka University, Osaka, Japan in 1981. Since 1972, he has been a professor in the School of Electronics, Telecommunication and Computer Engineering, Hankuk Aviation University, Kyounggi-Do, Korea. In Hankuk Aviation University, he was a dean of Student Affairs Division from 1989 to 1990, a dean of Academic Affairs Division from 1991 to 1992 and in 1996, a chief of Research Institute for Electronics, Information and Telecommunication from 1993 to 1996, a dean of Graduate School Aviation Industry from 1996 to 1998, and a dean of Graduate School from 1999 to 2002. He received the medal of Science Research in 1984, 1994, 1995, and 2002. His research interests are in the areas of wireless communication, mobile communication, and electromagnetic interference. He is a member of Korean Institute of Communication Sciences where he was a vice president in 1998, a member of Korea Electromagnetic Engineering Society where he was a vice president from 1996 to 2001, a member of Korea Navigation Institute where he was a president from 2001 to 2002, a member of Korea Institute of Maritime Information & Communication Sciences, a member of IEEE, and a member of IEICE(Japan).