Authentication & Accounting Mechanism on IEEE802.1x with Mobile Phone

Hyung-Woo Lee*
Div. of Computer, Information & Software
Hanshin University, Kyunggi, Korea

Kwang Moon Cho
Dept. of Electronic Commerce
Mokpo National University, Jeonnam, Korea

ABSTRACT

The number of wireless public network user is increasing rapidly. Security problem for user authentication has been increased on existing wireless network such as IEEE802.11 based Wireless LAN. As a solution, IEEE802.1x (EAP-MD5, EAP-TLS, EAP-TTLS), X.509, protocol or security system was suggested as a new disposal plan on this problem. In this study, we overview main problem on existing EAP-MD5 authentication mechanism on Wireless LAN and propose a SMS(Short Message Service) based secure authentication and accounting mechanism for providing security enhanced wireless network transactions.

Keywords: *Interaction with Wireless network, Authentication & Accounting, WLAN, SMS, EAP-MD5.*

1. INTRODUCTION

Internet had spread in all fields with the fast speed for last 10 years. Spread of Wireless network environment is supplied with the fast speed for the latest year. But, wireless network had tried quantitative swelling of wireless network service environment when wireless network business does not care greatly about security functionality commercially for the first time. As a result, form and technology of wireless network invasion are increasing number of times. Therefore, the variety succeeds attack attempt and invasion is also increased gradually as a proportional with time.

Current wireless network is supplying Message encryption and user certification mechanism for wireless MAC frame through WEP and WPA etc. to solidify security. Through RADIUS and DIAMETER protocol, wireless network is offering user authentication and improved services. However, send-receive through existent protocol is not secure because packet sniffing for overall frame is possible. One solution is to supplement domain and limitation of certification process through service that associate except existent radio frame.

In this study, we propose new protocol by associating SMS(Short Message Service) with existing RADIUS based authentication system for providing security enhanced and convenient one. The characteristics of protocol are personal information (privacy) protection and reinforcement by using the key given from SMS system. Also, we can implement easily the accounting system that is used in hand phone.

Certification way of existent wireless public network system delivers EAP-Request message to terminal including user information for transmit in AP on EAPoL packet. User terminal records EAP message including his own username on EAPoL packet and sends it to AP. And AP sends the message to RADIUS server. And RADIUS server notifies the result to AP that EAP Success message is received after examine whether RADIUS server had valid list in presented user account table. AP that receives this result is taking processes that permit internet access to relevant user.

At this procedure, the main issue is that username is exposed to malicious attacker. Username part that is stored in EAP message is transmitted to AP and RADIUS server when it is not encoded. We transmit sharable key to terminal through SMS between RADIUS server and terminal to supplement these limitation. And we propose protocol that encrypt and transmit EAP message by encrypt username using previously shared key by SMS.

In this study, we propose SMS based certification system based on ID/Password that is used in existent wireless public network. Presented system distributes secret key using AES-128 algorithm to user. And this secret key is used EAP certification procedure and EAP Message's encryption process. RADIUS server connects and achieves decryption process by using secret key that is created at user certification request process with user authentication server.

This paper explained about protocol that describe background

* *Corresponding author. E-mail: hwlee@hs.ac.kr*

Manuscript received Dec.15, 2006 ; accepted Dec. 29, 2006

This work was supported by the MIC, Korea, under the 2006 ITRC support program by the TTA(IITA-2006-(C1090-0502-0020)).

knowledge to understand proposed protocol in Chapter 2, and proposes advanced one in Chapter 3. And in Chapter 4, we propose a safe certification system through combination with proposed protocol. And certified method is reviewed for providing high performance through comparative analysis with existing certification system. Finally, we described about conclusion with future research topics in Chapter 5.

2. BACKGROUND

2.1 EAP-MD5 Authentication Mechanism

The MD5 authentication method[1] is the simplest one available to wireless LAN users, and support is required in the EAP standard. However, the security of MD5 in a wireless environment is so blatant, that some wireless vendors have chosen not to allow MD5 as an authentication method. With MD5 authentication, the authenticator sends a challenge to the supplicant: some string, along with a serial number. The supplicant proves it knows the password by hashing the challenge, the string, and the password together and then sending the information back.

Below Figure 1 shows the simplified IEEE802.1x EAP-MD5 mechanism. In first step, station connects with AP running certification procedure of system level by Open System or Shared Key Authentication. This connection is not more that Ethernet Station connects by cable in Switch. Since, run certification procedure of user level by EAP formality.

And then AP receives EAP-Request [Identity] message transmit user name if receive EAPoL Start message from terminal, or sense truth that terminal is connected to EAPoL Packet and require to terminal. Identity item of this case user name be instead of, name etc., of SSID and AP that is AP's information are received.

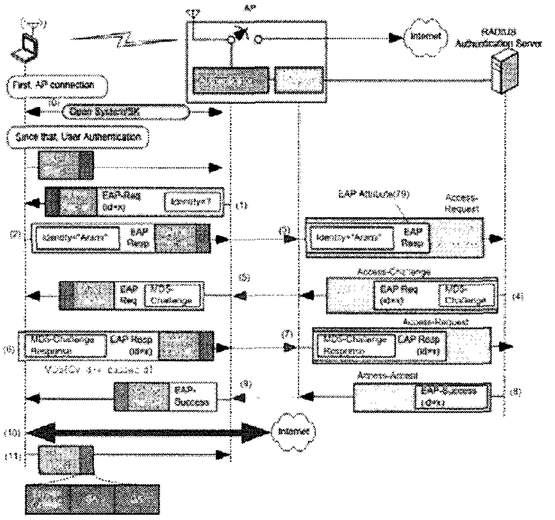


Fig. 1. IEEE802.1x EAP-MD5 Mechanism (EAP-MD5 Challenge)

AP creates RADIUS Access-Request message which is received EAP-Response [Identity] message from terminal. Then RADIUS Serve composes EAP Request message(MD5-Challenge Value (CV) : RADIUS Access-Challenge message) and send it to AP. After much more interaction between RADIUS server and Station, if Station receives EAP Success message, it can approach to outside(Internet) via AP[2].

Challenge-based authentication schemes, like MD5, were designed to counter the insecurity of schemes like PAP (Password Authentication Protocol), which actually send the username and password in the clear across the wire. With MD5 (or CHAP in traditional PPP), the password doesn't pass across the wire. Instead, the supplicant "proves" that it knows the password. MD5 is fine for dialup, but there are three issues that render MD5 less than optimal for wireless authentication.

First, MD5 requires that user passwords be stored in a way that lets the authenticator get at the original plain-text password. You'll sometimes hear this referred to as "reversibly encrypted." This opens up the possibility of someone other than the authentication server getting access to the file of passwords.

Secondly, MD5 only authenticates the supplicant. It does nothing to authenticate the authenticator, the wireless access point. Since wireless is especially vulnerable to impersonation, this is the major problem. Whereas impersonating a dial-up access server on the other end of a phone line is fairly difficult, impersonating wireless just means getting within a couple hundred feet of the supplicant. This lack of mutual authentication is the reason some wireless vendors have chosen not to allow MD5.

Thirdly, MD5 does not create a WEP session key. Ideally, immediately after authentication, the wireless client and access point would jump into WEP-encrypted communications, which reduces the risks of eavesdropping, impersonation, or data corruption by a hostile attacker. Other authentication methods, such as TLS and TTLS, support this but MD5 does not and therefore this limits its usefulness in the wireless world. Table 1 shows the basic summary and comparison results on detailed mechanism used in existing EAP mechanism

Table1. Common EAP Authentication Methods

Method	WEP Key Generated ?	Deployment Difficulty	Wireless Security
MD5	NO	Easy	Poor
TLS	YES	Hard	Best
TTLS	YES	Moderate	Better

One WEP flaw is based upon what is called an 'IV collision'. An IV(Initial Vector) collision simply means that an IV is reused at some point in a wireless transmission. Recall that an IV is added to the secret key in each packet to ensure that each packet has a different RC4 key, given that the secret key doesn't change frequently. A well-known problem with stream ciphers is that two packets encrypted with same IV can be easily[3]. The equations below demonstrate algebraically how the attack works. Table 2 shows the weakness on WEP protocol.

Table2. Weak Key on WEP Protocol

$$C_1 = P_1 \otimes RC4(k,v)$$
$$C_2 = P_2 \otimes RC4(k,v)$$
$$C_1 \otimes C_2 = (P_1 \otimes RC4(k,v)) \otimes (P_2 \otimes RC4(k,v))$$
$$C_1 \otimes C_2 = P_1 \otimes P_2$$

The first and second equations show that two ciphertexts (*C*1 and *C*2) are calculated by XORing the plaintext (*P*1 and *P*2) and the same keystream *RC4*(*v*,*k*), where *v* is the IV and *k* is the secret key. A little algebraic manipulation demonstrates that two ciphertexts that use the same keystream (i.e., *RC4*(*v*,*k*)) cancel the keystream, resulting in the XOR of the plaintexts: *P*1 Ä *P*2 (Borisov, Goldberg, & Wagner, 2001).

Attackers have several avenues for partitioning the two XORed plaintexts. One way is through the use of a known plaintext attack. If an attacker can get a victim to send known plaintext, such as spam or through an email, then it is fairly trivial to recover the unknown part of the XORed plaintext message.

Also, the probability that an attacker is able to infer plaintext in a message is fairly good given that IP traffic is structured in a well-known manner, e.g., there is consistent information in the TCP and UDP headers across packets. Failing this, some understanding of the statistical nature of repetition of letters in an alphabet and some common sense may led to an attacker's partitioning of the two plaintext messages.

IV collisions are all but ensured by several factors. First, the 24-bit IV keyspace is not large enough to ensure against collisions for any reasonable length of time.An AP that sends 1500 byte packets at 11Mbps will exhaust the keyspace of IVs in as little as five hours.

Second, some wireless NICs reinitialize IVs to 0 each time a card is initialized and increments by 1 for each packet. This means that transmission begins with a known and repeating IV, resulting in the opportunity for more IV collisions or allowing attackers to guess the IV.

Third, WEP security is based on the assumption that secret keys are changed on a frequent basis. In reality, secret keys are not changed on a frequent basis, largely because it's a manual process and time consuming: the key must be distributed and inputted into each user's software, as well as the AP. And it is unlikely that anyone would change keys every five hours. Based on these factors it is almost a certainty that collisions occur frequently.

2.2 Vulnerability of EAP-MD5 Authentication Mechanism

Certification system (EAP-MD5) based on PAP system has many limitations. First, EAP-MD5, the original implementation of EAP, is vulnerability to man-in-the-middle attack–referred to as MITM or monkey-in-the-middle-attacks(taken from a popular MITM tool called monkey_jack[5]) against the AP because there is no AP/server-to-host authentication.

A rogue AP placed between the EAP-MD5 supplicant and the RADIUS server can easily snatch the users employing sent to the authentication server and even authenticate users employing false credentials[6].

Second, Because Message encryption does not consist in EAP-MD5 Wireless torso that increase, is weak in hackers' Sniffing attack. And EAP-MD5 certification way uses MD5 Hash function to this Hash function too much limitations find [7]. Figure 2 shows the overall mechanism of EAP-MD5 and its vulnerability.

We propose PAP base certification system that uses SMS to prevent these limitations. Proposed system combines existing mobile phone service with wireless public network account service.

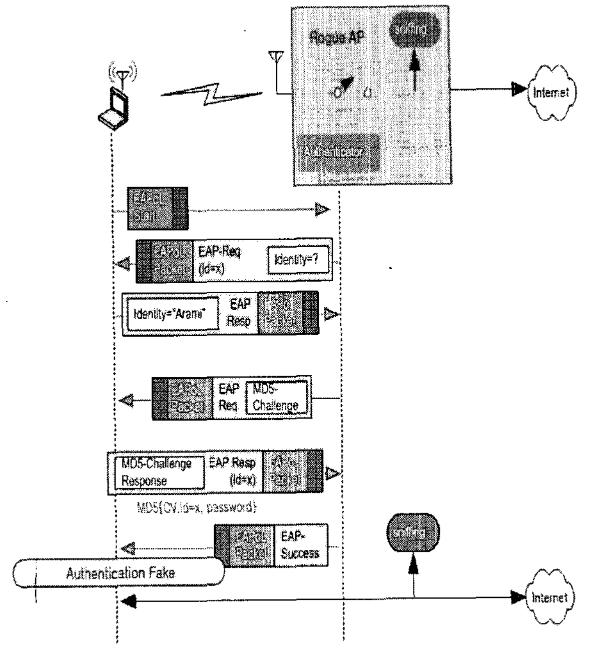


Fig. 2. EAP-MD5 Vulnerability

2.3 Advanced Encryption System (AES)

Rijndael is designed for use with keys of lengths 128, 192, and 256 bits. First, We give a brief outline of the algorithm, then describe the various components in more detail.

The algorithm consists of 10 rounds. Each round has a round key, derived from the original key. There is also a 0th round key, which is the original key. A round starts with an input of 128 bits and produces an output of 128 bits.

There are four basic steps, called layers, that are used to form the rounds[3]:

- The ByteSub Transformation: This non-linear layer is for resistance to differential and linear cryptanalysis attacks.
- The ShiftRow Transformation: This linear mixing step causes diffusion of the bits over multiple rounds.
- The MixColumn Transformation: This layer has a purpose similar to ShiftRow.
- AddRounKey: The round key is XORed with the result of the above layer.

Putting everything together, we obtain the following [Table 3]:

Table 3. Rijndael Encryption

Rijndael Encryption
1. RK, using the 0th round key.
2. Nine rounds of BS, SR, MC, ARK, using round key 1 to 9.
3. A final round: BS, SR, ARK, usong the 10th round key.

The final round uses the ByteSub, ShiftRow, and AddRoundKey steps but omits MixColumn (this omission will be explained in the decryption section) The 128-bit output is the ciphertext block.

3. SMS BASED SECURE AUTHENTICATION & ACCOUNTING SYSTEM

3.1 SMS based Secure Authentication

New SMS based certification system can provide stable wireless public network service. It can solve the vulnerability problems on EAP-MD5 certification system and also can provide message encryption on wireless transaction as follow Figure 3.

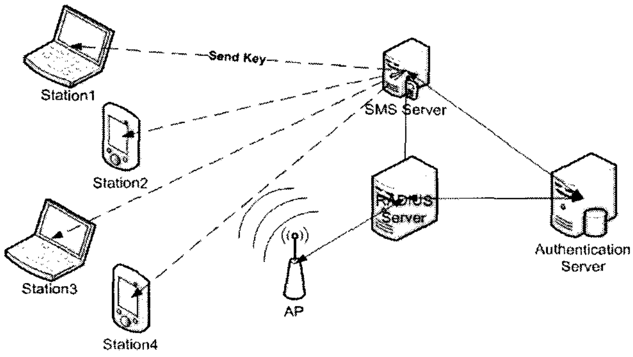


Fig. 3. Model of SMS based Security Authentication System

3.1.1 EAPoL Frame on Station

On SMS based PAP certification system, each Stations encrypts their own EAP packet using AES algorithm with Secret Key that is received by SMS message from SMS server. In this time, each entity receives EAP packet on EAPoL frame which is prescribed in 802.1x for data transmission on wireless transaction. EAPoL frame structure is shown in Figure 4. EAP packet on EAPoL frame is used for security enhancement on wireless transaction and it contains the most important user information(User ID and Password), which is used in certification process between the Station and RADIUS Server. Encryption process executes encryption on EAP Message using AES algorithm using 128 bit key.

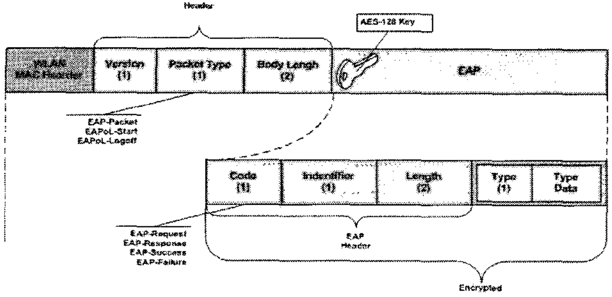


Fig. 4. EAPoL Frame Format

3.1.2 SMS based Authentication through AP

AP delivers frame between Station and RADIUS Server. A specific implication of man-in-the-middle attack is performed by a Rogue AP. It attacks one-way IEEE802.1x authentication mechanism which is based on EAP-MD5. To perform such an attack, Rouge AP will impersonate as a Rogue RADIUS Server by providing fake credentials in the form of always positive authentication reply to the station.

Therefore we propose an efficient defense mechanism against this vulnerability as follow Figure 5. User encrypts and sends an EAP packet using secret key that is received from AP. And then authenticated RADIUS server can decrypt message included in EAP packet.

As shown in Figure 5, each station that receive EAP-Request [Identity] message from AP transmits EAP-Response message as a response message. Station receives his own information from the RADIUS Server through AP.

RADIUS Server that receive EAP-Response message (UserID) creates 128bit secret key that do Random. At this time, SMS Server *transmits* Secret Key *to* the user's Hand Phone by SMS message after comparing the user's information with that is stored in user authentication table on Authentication Server.

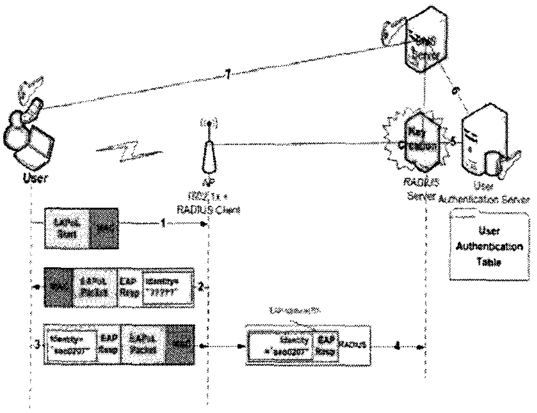


Fig. 5. Secret Key Distribution on SMS Message

RADIUS Server is system that act important role that take charge decision of certification success availability and Secret Key relationship creation function in this system. RADIUS Server that accept user's ID information reads Hand-Phone information of use in User Authentication Table and give Secret Key transmission command by SMS Server. By this mechanism, we can get some effectiveness. We can keep away user's partial secret from the wired network. As the secret key is received from the SMS message, we can construct the secret sharing mechanism on the ID/PASSWORD based authentication mechanism.

Station creates hash value with user's own password, CV and seq_ID. Station transmits EAP packet including created hash value to RADIUS Server. And then RADIUS server also creates HV' using password that is stored already on his own account table and CV and seq_ID. Finally, RADIUS Server compares received HV ' value with computed HV value. Of course, encryption on EAP packet is achieved independently with commonly used MD5 hash function in this process.

User authentication table is situated to Authentication Server. It is place that necessary user information is stored in certification process of RADIUS Server and each Station on this table. Secret Key that is created in RADIUS Server is stored to Authentication Server's Secret Key field.

User data is used in Authentication Server. User information is stored in certification process of RADIUS Server and each Station. Secret Key that is created by RADIUS Server is also stored to Authentication Server's Secret Key field. Secret Key is updated every time if required. For example, we can construct user information lookup table as follow Table 4.

Table 4. User Information Table (For Example)

Identity	PW	HP	Secret Key
Seo0207	*********	016) 395-xxxx	128bit
Je3309	*********	011) 740-xxxx	128bit
aiking	*********	010) 234-xxxx	128bit
Lily0405	*********	019) 362-xxxx	128bit

3.2 SMS based Accounting Mechanism

Current wireless public network users can be connected to public network after preliminary registration are given based on ID and Password authorization process. Also, users pay money according to connection time. But, present wireless network environment can not use network in all time and places that users want. By various kinds factor, there is a case that smooth service is not achieved. This time, existing subscribers can feel many discomforts. And network administrator also has present complaint in fare system of wireless network that make fixed amount of money and then use unlimited connection mode.

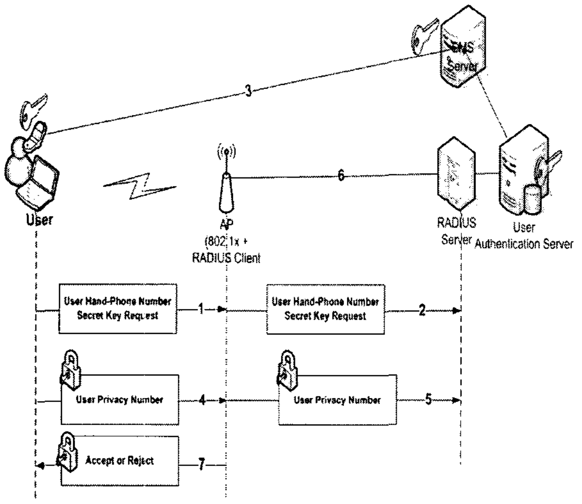


Fig. 6. SMS based Accounting Process

As above Figure 6, we can solve these users' discomfort. User who do not join in Wireless public network service transmits his own Hand-Phone number and Secret Key request message to Radius Server, and RADIUS Server transmits Secret Key to user Hand-Phone using SMS. Secret Key of user is given and encrypts individual's unique number (resident registration number Korean case) by Secret Key and transmits to RADIUS Server with joined beforehand user.

RADIUS Server that accepts user information foretells availability whether Hand-Phone subscriber's unique number and unique number that request person inputs conform. If these input two values equal, user can use wireless network service.

4. EXPERIMENTATION & ANALYSIS

4.1 Experimentation Environment

Experiment of this scheme is shown in Figure 7. In an experimental result, we can see actual packet of EAP-MD5 after certification process and we can view real packet contents after analyzing about the proposed techniques that is encoded by Key value drawn from SMS Server, by which we can see the enhanced contents compared with existent system. Station's experimental environment is based on Windows XP, AP used LinkSys WRT54GS Access Point. We use RADIUS Server on Windows 2003 operating system and test this module with AES-128 Key's encryption process on Matlab 7.1.

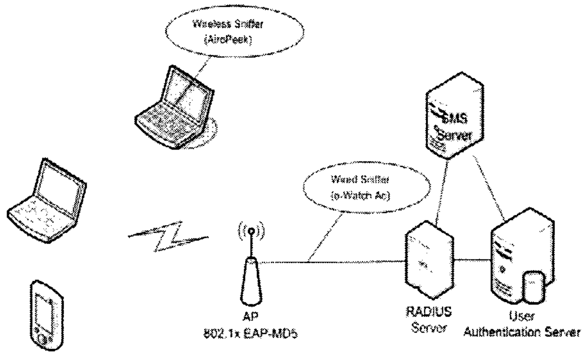


Fig. 7. Experimentation Environment

4.2 Rogue AP Protection

EAP message is recorded on EAPoL frame and it is also transmited to the receiver. EAPoL frame is consisted of Protocol Version (1 byte), Packet Type (1 byte), Body Length (1 byte) and EAP message.

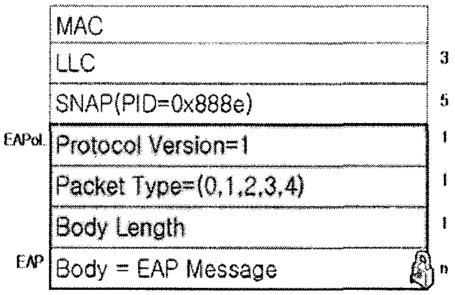


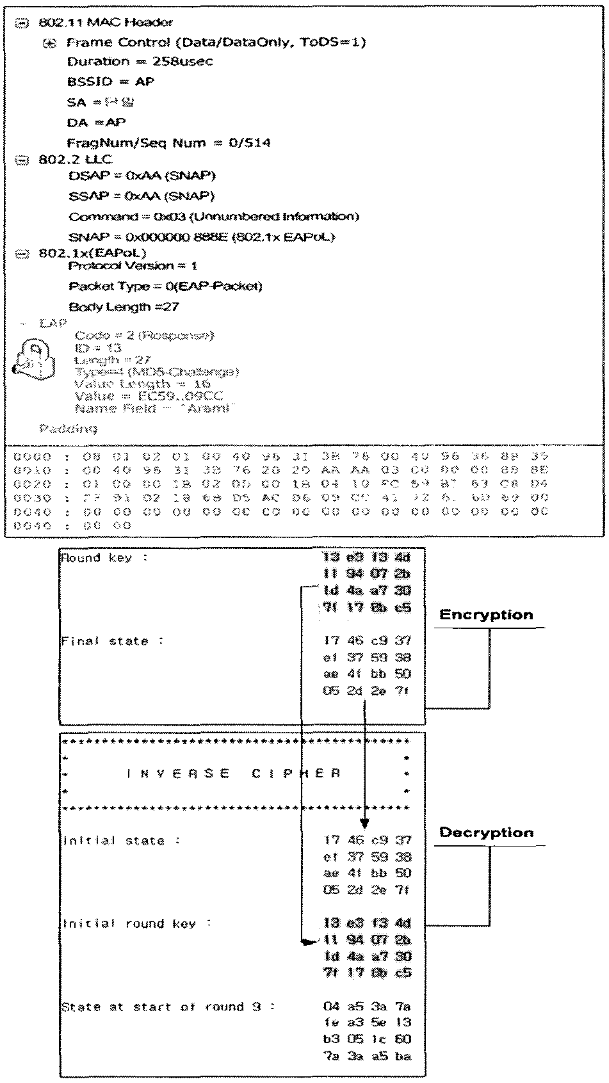
Fig. 8. Frame Form of EAPoL

As shown in Figure 8, EAPoL frame is consisted of fixed Packet length. And we can detect rogue AP by using encrypted

EAP message on EAPoL frame. Attack by rogue AP is possible because there is no mutual authentication process. Rogue AP sends a message EAP-Success message to Station, Rogue AP that do not know Secret Key of Station and RADIUS Server can not encryption EAP-Success message. Rogue AP gives Secret Key to Station using SMS Server. However, it is impossible to see user's ID information and can't know user's Hand-Phone number.

4.3 SMS based EAP-Message Encryption/Decryption

Figure 9 shows a frame sniffing result. EAP Message's frame structure can know in Figure 8. EAP Header part has 4byte's data frame all, and data of Body Type's 1byte and real EAP of Type data of EAP Body part is received. This paper encrypts EAP message entirety (header inclusive).



```
⊟ 802.11 MAC Header
   ⊞ Frame Control (Data/DataOnly, ToDS=1)
     Duration = 258usec
     BSSID = AP
     SA =단말
     DA =AP
     FragNum/Seq Num = 0/514
⊟ 802.2 LLC
     DSAP = 0xAA (SNAP)
     SSAP = 0xAA (SNAP)
     Command = 0x03 (Unnumbered Information)
     SNAP = 0x000000 888E (802.1x EAPoL)
⊟ 802.1x(EAPoL)
     Protocol Version = 1
     Packet Type = 0(EAP-Packet)
     Body Length =27
 - EAP
      Code = 2 (Response)
      ID = 13
      Length = 27
      Type=4 (MD5-Challenge)
      Value Length = 16
      Value = EC59..09CC
      Name Field = "Arami"
   Padding

0000 : 08 01 02 01 00 40 96 31 38 76 00 40 96 36 89 35
0010 : 00 40 96 31 38 76 20 29 AA AA 03 00 00 00 88 8E
0020 : 01 00 00 1B 02 0D 00 1B 04 10 EC 59 87 63 C8 D4
0030 : 77 91 02 18 68 D5 AC 06 09 CC 41 72 61 6D 69 00
0040 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 : 00 00
```

```
Round key :                              13 e3 13 4d
                                         11 94 07 2b
                                         1d 4a a7 30
                                         7f 17 8b c5

Final state :                            17 46 c9 37
                                         ef 37 59 38
                                         ae 4f bb 50
                                         05 2d 2e 7f
```

```
***********************************************
*                                             *
*       I N V E R S E   C I P H E R           *
*                                             *
***********************************************

Initial state :                          17 46 c9 37
                                         ef 37 59 38
                                         ae 4f bb 50
                                         05 2d 2e 7f

Initial round key :                      13 e3 f3 4d
                                         11 94 07 2b
                                         1d 4a a7 30
                                         7f 17 8b c5

State at start of round 9 :              04 a5 3a 7a
                                         fe a3 5e 13
                                         b3 05 1c 60
                                         7a 3a a5 ba
```

Fig. 9. EAP Encryption & Decryption Result

5. CONCLUSION

By using these new protocol, we can construct secure system compared with existing EAP over LAN(EAPoL). The reason is that a user's ID was encrypted by the previously shared key after receiving a SMS message. User who is not joined in wireless public network can connect easily and authenticated securely to it with accounting system through hand phone.

We instituted problem about Rogue AP by certification absence between EAP-MD5 base wireless certification systems. Also, we indicated elements of EAP Message encryption process in wireless authentication to controversial point. As a improvement way, we presented method to distribute secret key to users using SMS. And we developed EAP-Message encryption module with AES-128 encryption algorithm using these shared secret key. As a result, we can prove that secure authentication process is possible on wireless environment with proposed SMS based mechanism.

For future works, we can combine wireless authentication mechanism with fingerprint certification procedure. Using it, we can propose certification system that use fingerprint to solve authentication problem happen in existing wireless certification system. Therefore, we will supplement security vulnerability in existing wireless certification system.

REFERENCES

[1] Wireless LAN Security Interoperabillity Lab, "**What are EAP Authentication**", pp. 1-2.

[2] Jong-Ho Yoon, "**Wireless LAN Security Protocols**", pp. 282-283, 2005.08.

[3] J. Phillips Craiger, "**802.11, 802.1x, and Wireless Security**" 2002.06.

[4] Wade Trappe, Lawrence C. Washington, "**Introduction to CRYPTOGRAPHY with CODING THEORY**", Prentice Hall, pp.128-136, 2001.03.

[5] Kevin Beaver, Peter T.Davis, "**Hacking Wireless Networks for DUMMIES**", WILEY, pp.208, 2005.

[6] Andrew A. Vladimirov, Konstantin V. Gavrilenko, Andrei A. Mikhailovsky, "**Wi-Foo**", Addison-Wesley, Fifth printing, pp.182, 2005.10.

[7] Xiaoyun Wang, Hongbo Yu(Shandong University), "**How to Break MD5 and Other Hash Function**".

[8] Jorg J. Buchholz "**Matlab Implementation of the Advanced Encryption Standard**", http://buchholz.hs-bremen.de, 2001.11.

Hyung-Woo Lee

He received the B.S., M.S. and Ph.D. degrees in Computer Science from Korea University in 1994, 1996 and 1999, respectively. From 1999 to 2002, he was an assistant professor in the Division of Information and Communication Engineering, Cheonan University. He is currently an associate professor in the Division of Computer, Information and Software, Hanshin University, Korea. His research activities are mainly in the areas of information security, network security, and wired/wireless IDS/IPS.

Kwang Moon Cho

He received the B.S., M.S and Ph.D degrees in computer science from Korea University, Korea in 1988, 1991 and 1995 respectively. From 1995 to 2000 he was with Samsung Electronics Research Center where he worked on developing telecommunication softwares. From 2000 to 2005 he was with Cheonan University where he worked as a professor of the division of information and communication engineering. In 2005, he joined Mokpo National University where he is a professor of Electronic Commerce major. His main research interests include electronic commerce, communication software, mobile content and grid computing.