A Scheme for Improving WEP Key Transmission between APs in Wireless Environment*

Chi Hyung In, Choong Seon Hong, and Il Gyu Song

School of Electronics and Information, Kyung Hee University
1 Seocheon, Giheung, Yongin, Gyeonggi 449-701 KOREA
inchihyung@hanmir.com, cshong@khu.ac.kr, songilgyu@hanmail.net

Abstract. Wireless LAN (WLAN) refers to the wireless network environment constructed indoors or outdoors, by using either the radio or light wave technology instead of wire signals from the hub to such clients as PCs (Personal Computer), notebook PCs and PDAs. TGf (Task Group F), among IEEE 802.11 WGs (Working Groups), is currently under formulation of the standard protocols for communication between WLAN Access Points (APs). This Group has proposed IAPP (Inter Access Point Protocol) designed to secure the interoperability between AP sets produced by different vendors. This is a protocol for securing mobility among APs within sub-networks. It offers seamless connectivity between stations (STAs) by sharing security context or Layer 2 forwarding data between APs without re-authentication when STAs move around among them. In this paper, we propose a mechanism to enhance the wireless LAN security protection related information as WEP key that can occur during message transmissions between APs by replacing the movement paths for IAPP move requests or response messages with the existing movement path utilizing the public key for transmission between above APs.

1 Introduction

802.11 wireless LAN[1] is a technology that started with the increase of Internet users and the development of wireless communication technologies. As IEEE published its 802.11b standard for the wireless LAN, the WLAN market has grown rapidly. The standard did not define any specific methods as there can be diverse methods that can materialize WLAN system concepts. This resulted in flexibility and diversity among AP designs by the individual vendors but made it difficult for the APs to interoperate with each other. To address this problem, TGf proposed IAPP (Inter Access Point Protocol)[2] to have the interoperability among APs from different vendors. IAPP is a protocol that is designed to secure mobility among different APs, enabling STAs to speedily move by sharing data among the APs. However, the openness property of wireless media has aroused the problem of hacking, against which it is essential to set up a security system.

* This work was supported by University ITRC Project of MIC. Dr. C.S. Hong is the corresponding author.

A. Laganà et al. (Eds.): ICCSA 2004, LNCS 3043, pp. 792–801, 2004.

IAPP uses ESP (IP Encapsulating Security Payload)[4] for the security of data among APs. However, many different problems have recently resulted from key protection. This paper propose that the move path of shared data should be replaced to protect of data that may arise in sharing data among APs to enable the speedy mobility of STAs and also a new scheme that the public key should be used for secure key transmission in the wireless sections. This paper is configured as follows: Chapter 2 includes a related study of wireless LAN, Chapter 3 introduces the basic authentication method under 802.11b, Chapter 4 reviews the architecture and mechanism of the existing IAPP protocol, Chapter 5 proposes the method for securing message security in forwarding data among APs and also evaluates its performance, and Chapter 6 provides the conclusion.

2 Related Works

2.1 Current Study of Wireless LAN

As 802.11 standards were originally ratified in 1997, there have been various proposals for their improvement. 802.11a[6] offers a bandwidth five times wider than that offered under 802.11b standards, and 802.11g is also expected to be introduced soon. The security is the biggest concern the network administrator faces in designing and implementing a wireless LAN. In the wired network environment, we can block unauthorized or rogue accesses to the internal network by limiting the physical channels. In the case of the wireless LAN, however, we cannot tell where the wireless device user is located - inside the building, in the lobby or outside the building. Under IEEE 802.11, it was known, data transmission over an unreliable wave eventually induces snooping. Therefore, they introduced three approaches to enhance the security of data passing the wireless LAN sections. The first is to use 802.11 SSID, and the second is to authenticate wireless devices based on MAC addresses. The third is to use WEP (Wired Equivalent Privacy) key. The MAC address based approach is to authenticate access requests by comparing the requesting party with the lists stored within the AP or in an external database. In other words, only the users whose identity matches the stored lists may succeed in accessing the wireless network. This approach is advantageous on a small size network. The following chapter will provide a detailed explanation of SSID and WEP.

2.2 Basic Authentication Scheme under 802.11b

IEEE 802.11b wireless LAN technology[9], which is widely used these days, has the following mechanism: When a STA sends access request to a nearby AP to access the wireless network using a mobile LAN device, the AP interfaces with the STA using an authentication server called RADIUS (Remote Authentication Dial-In User Service)[3]. The access processes are shown in Figure 1.

The current 802.11b standards define SSID (Service Set IDentifiers) and WEP (Wired Equivalent Privacy) to support the wireless LAN user authentication and privacy. SSID provides the basic level access control means. They

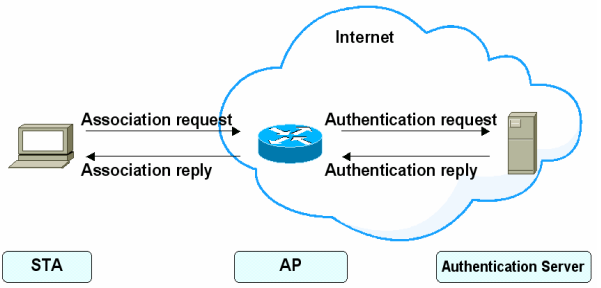

Fig. 1. STA User's Network Access Processes

are the network names for wired LAN devices, utilized when the network is separated into segments. SSID is the number used to divide the logical domains on the wireless LAN. Being high vulnerable security-wise, the wireless LAN set up solely with SSID would have many security problems. SSID based access control is included in Probe, the reply message to Probe, the request message transmitted by the terminal device for initial access or is included in the beacon message regularly broadcast by the AP. The basic authentication is performed using the SSID included in such messages, with which the system controls terminal device attempts for access by recognizing it. SSID is related to one or more APs to create multiple wireless LAN segments in the infrastructure BSS (Basic Service Set). The segments are related to the building floor, business unit or data definition set. SSID works as the default password as its original form appears during the authentication process. As the wireless terminal equipment is generally set up by the end users, the SSID is shared among the users, degrading the security effectiveness. Another inconvenience in using the SSID for authentication is that the SSID of all the wireless equipment and APs should be changed whenever a SSID is changed. In this connection, WEP (Wired Privacy Equivalent) encryption provides a more effective security to the data. WEP provides a mechanism to protect data stream on the wireless network by using a symmetric encryption algorithm. Therefore, it uses an identical key and algorithm for encoding and decoding. The user access request is denied when authentication fails with a wrong WEB key. This approach also involves some problems. As an identical key is used for encoding and decoding and the same algorithm is shared by the terminal device and APs, it is difficult to control keys when distributed or shared. As the keys are controlled statically, it is difficult to distribute them. It has the defect of degraded security. To address this problem, IEEE802.11i Group [7] has proposed WEP2, which enhances security by making the existing WEP key longer and also proposed RSN (Robust Security Network).

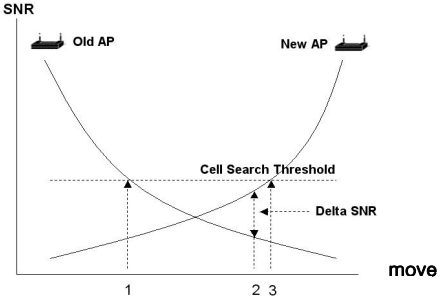

Fig. 2. Starting Point of Terminal Roaming

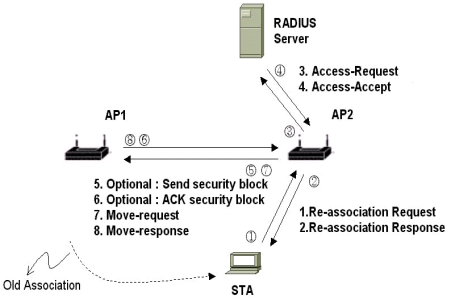

Fig. 3. IAPP Operation Process

3 IAPP Protocol

3.1 IAPP Protocol Structure

IAPP is initialized while exchanging IAPP-INITIATE service primitive through APME (AP Management Entity) and IAPP SAP (Service Access Point) which are AP operational entities characterized by AP features and functions. IAPP uses RADIUS clients to support 802.1x authentication[5] when it receives STA request for reset through APME. Clients perform mapping of AP BSSID and IP addresses and key distribution for encryption among the APs by communicating with RADIUS server. - APME : IAPP Management Entity

- IAPP : Inter Access Point Protocol
- ESP : IP Encapsulating Security Payload
- DSM MAC : Distribution System Medium MAC
- WM MAC : Wireless Medium MAC

3.2 Roaming Process of Wireless Terminals

Mobile wireless terminals roam by comparing the newly received SNR value with the current connection SNR value. At this time, the signal level is obtained by

the beacon message generated by all the APs. SNR value is also called "Cell Search Threshold". It needs the re-association process and a mobile wireless terminal needs connection with the AP. The re-association process starts when SNR value falls below the threshold value. The mobile wireless terminal starts the re-association process with a new AP when the difference between the current SNR value and the newly received SNR value is larger than the threshold value, also called the delta SNR. Figure 2 shows a table comparing the SNRs for determination of mobile wireless terminal roaming. SNR value can be obtained at a given location from two APs. If the wireless mobile terminal moves to the right, the SNR value from the previous AP will decrease. It comes closer to the new AP and the SNR value increases at same time. If SNR value falls below Cell Search Threshold value, the mobile terminal starts Cell Search mode to search an active channel. If it moves further to the right, the SNR value of the new AP increases even larger than that of the previous AP. Yet, it is not connected to the new AP. Roaming starts when the SNR value difference between the new AP and the previous AP gets larger that the delta SNR value. Cell search mode is maintained until the SNR value increases over Cell Search Threshold value. Movement in the reverse direction will go through the same process from the new AP to the previous AP.

3.3 IAPP Mechanism Overview

IAPP is a protocol that is designed to ensure mobility among APs on a sub-network. It provides the speedy mobility to terminals by sharing Layer 2 Forwarding and Security Context data between APs. IAPP operates in the environment that includes multiple APs, mobile stations, distribution system, and one or more RADIUS servers. It uses ESP as the security algorithm to relay WEP keys between two APs. It gets ESP authenticator from RADIUS, the authentication server. Message data flows between the AP and the terminal on a same sub-network that supports IAPP as shown in Figure 3. STA requests AP2 for reset when it enters the latter's domain. If AP2 uses Proactive Caching[8], APME first searches the terminal's context data in IAPP cache using the terminal's MAC address. When it finds a context data in the cache that matches the terminal's data, it can speedily hand off by directly using the cache data. If it fails to find a context that matches the terminal data, it goes through the existing hand-off process as shown in Figure 3. RADIUS Access accepting message includes ESP authenticator data that is the algorithm for encoding the Move request and its reply message exchanged between AP1 and AP2. Recently, the messages exchanged between AP1 and AP2 and the WEP key and passwords designed for privacy between STAs and APs are exposed to higher threats by malicious hacking sources. Further, APs that do not support IAPP may experience poor connection with APs that support IAPP.

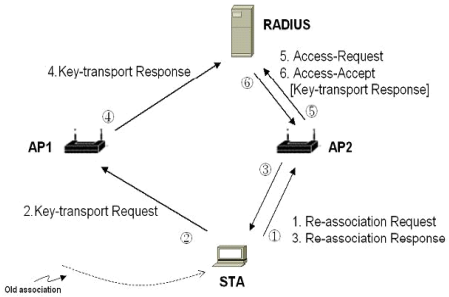

Fig. 4. STA Moves from AP1 toward AP2

4 Proposals and Solutions

4.1 Proposals

This paper proposes solutions of using the already authenticated path between AP1 and the authentication server instead of the message path between AP1 and AP2 to reduce the possible leaks of confidential data and to address the poor connection problem between APs that support or do not support IAPP. It also propose to enhance the wireless LAN security by utilizing the public key. The mechanism of the proposed message transmission solution is illustrated in figure 4. When STA enters the domain of AP2, a new AP, it first sends a reset request message to AP2 referring to the parameters by receiving the beacon message regularly broadcast by AP2. AP2 sends a reset reply message in response to the STA message. STA then recognizes AP2 using the prefix data of AP2's beacon message. It than sends to AP1 a key-request message comparable to the existing Move request message. AP1 that receives the message sends a key-transport reply message comparable to the existing Move reply message to the authentication server, which in turn sends the Access-accept message to AP2. The Access-accept message includes the Key-transport reply message. AP2, a new AP that has received the message, is authenticated and will be able to obtain the WEP key from AP1, the previous AP. If AP2 fails to receive a reply message to the Key transport request message (Message No. 2), it will make several more attempts as in the general packet retransmission. If it still fails to receive the message, it will start a new authentication process just like the initial re-authentication process. The public key is used for the security of the wireless section between a STA and an AP. The public key used for this process is included in the certificate exchanged with the authentication server for initial authentication. Therefore, it is no longer necessary to obtain the public key separately. Thus, the security is enhanced for the wireless section that employs the public key. As STA connects two APs by recognizing them, the connectivity between them is enhanced. The solution proposed in this paper emphasizes the hacking of messages is better blocked by transmitting the confidential message and key data using a path that

is already authenticated rather than the use of the public key. By using this solution, we can achieve a performance similar to the proactive cache method newly proposed in Draft 5.0. In so doing, it will also reduce the cache work burden to the APs. For this solution, a new message format with command field No. 7 and 8 added to the existing packet are proposed as shown in Figure 5 and 6.

Address Length	Reserved	MAC Address	Sequence Number	Length of Context Block	Context Block
Octet : 1	1	n = Address Length	2	2	m = Length of Context Block

Fig. 5. Key-transport Request

Address Length	Status	MAC Address	Sequence Number	Length of Context Block	Context Block
Octet : 1	1	n = Address Length	2	2	m = Length of Context Block

Fig. 6. Key-transport Response

The current standard defines command fields up to No. 4 and the draft 5.0 newly defines No. 5 and 6. Fields No. 7 to 255 are reserved for future use. The author has defined key-transport request message in field No. 7 and key-transport response message in field No. 8(figure 5, 6). The author has also assigned Key-transport response message to 192 out of the RADIUS Access-Accept Attribute range 192 to 223 reserved for use by developers to insert key-transport response in the RADIUS Access-Accept message as shown in figure 8.

4.2 Measurement Outcome

This paper is to propose a solution targeted at protection of confidential messages such as WEP key etc. by detouring the message transmission path. Therefore, the author has evaluated its feasibility by measuring the overall delay experienced when the message transmission path is detoured to a more secure path. The test environment and results based on a simulation are as follows: OPNET8.0 simulator was used on Pentium 800 CPU computer using Windows 2000 OS, bandwidth of 10Mbps, delay of 5ms in wired LAN, and bandwidth of 1Mbps,

Value	Command
0	ADD-notify
1	Move-notify
2	Move-response
3	Send-Security-Block
4	ACK-Security-Block
5	CACHE-notify
6	CACHE-response
7	Key-transport-request
8	Key-transport-response
9 - 255	Reserved

Fig. 7. Command field value

Attribute number	Attribute Name	Value
1	User Name	Old BSSID
8	Frame IP Address	Old BSSID IP Address
...	...	...
80	Message-Authenticator	RADIUS Message's Authenticator
192	Key transport	Key-transport response

(Value 192-233 are reserved for experimental use)

Fig. 8. RADIUS Access-Accept Attribute

delay of 20ms in wireless environment. First, the utilization was measured to check the bandwidth consumption rate, and End-to-End Delay was measured to evaluate the overall performance as shown in figure 9,10.

The simulation test shows the solution proposed in this paper is believed to get the WEP key faster as it sends the key-transport request message, comparable to the Move-request message, at the same it sends the reset request message to relay the Move-request message. The solution provides a communication performance that is evaluated to be slightly poorer than the existing IAPP scheme. It is analyzed that the overall overhead is increased by the use of the public key. However, it can block hackers from capturing messages in transmission between

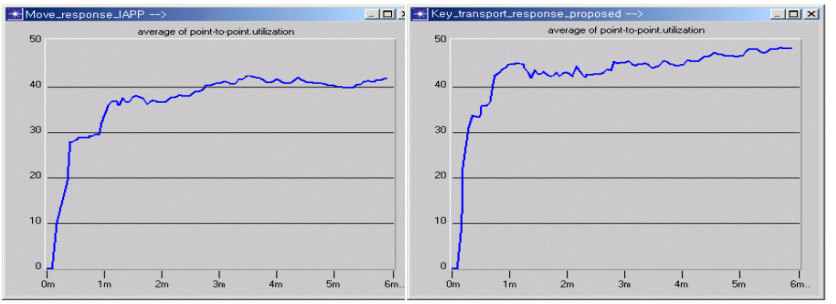

Fig. 9. Utilization measurement (Existing vs Proposed)

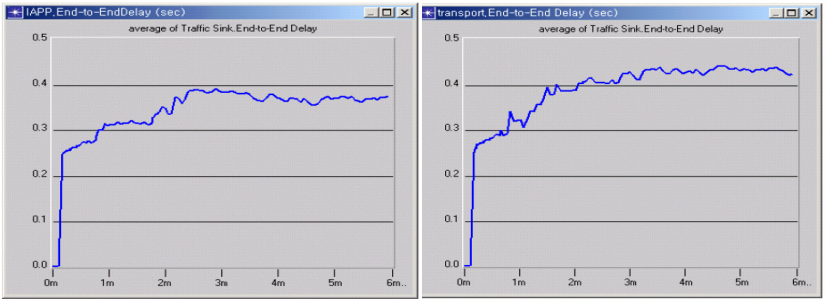

Fig. 10. End-to-End Delay measurement (Existing vs Proposed)

APs. It also offers a merit that the security is enhanced with the public key used to transmit the key on the wireless section between STA and AP.

5 Conclusions

Protection of WEP key and other confidential data exchanged between APs, this paper proposes the message transmission path should be diverted to the path that is already authenticated. It also proposes that the public key should be used to enhance the security of key transmission in the wireless section. This is expected to prevent the data exchanged between two APs from being exposed to malicious hacking. It will also provide a faster connectivity by sending the key-transport request message along with the reset request. It is also expected that the AP caching overhead would be reduced if a comparable throughput can be achieved without using the proactive cache mechanism newly proposed in 802.11f / Draft 5.0.

References

1. ANSI/IEEE Std 802.11, "Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specification," 1999.
2. IEEE 802.11f/D3.0 (Draft Supplement to IEEE 802.11, Edition): "Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation".
3. RFC 2865, "Remote Authentication Dial In User Service (RADIUS)", June.2000.
4. RFC 2406,"IP Encapsulating Security Payload(ESP)", November 1998.
5. IEEE Draft P802.1X/D11, "Standard for Port based Network Access Control," IEEE, Mar.2001.
6. IEEE 802.11a, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specification : High-speed Physical Layer in the 5GHz Band", 1999
7. IEEE 802.11i-D2.0, "Draft-Wireless Medium Access Control (MAC) and physical layer (PHY) specification : Specification for Enhanced security", March. 2002.
8. IEEE802.11f/D5.0 (Draft Supplement to IEEE 802.11, Edition): "Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation".
9. D. Nessett, "Serial Authentication Using EAP-TLS and EAP-MD5", IEEE, 802.11-01/400r22, July 2001.