A Study of User Authentication Protocol Considering the Mobility Based on IPv6 in a Wireless LAN Environment

Tae-Sub Kim¹, Ryong Oh¹, Sang-Joon Lee¹, Yi-Kang Kim¹, Byung-Bog Lee², Choong-Ho Cho¹,

¹ Department of Computer and Information Science, Korea University
{ree31206, orionpia, leesj1124, kimyikang, chcho}@korea.ac.kr
² Electronics and Telecommunications Research Institute
Bblee40@etri.re.kr

Abstract. – Wireless LAN (WLAN) refers to the wireless network environment constructed indoors or outdoors, by using either radio or light wave technology instead of wire signals from the hub to such clients as PCs (Personal Computers), notebook PCs and PDAs. TGf (Task Group F), among IEEE 802.11 WGs (Working Groups) has proposed IAPP (the 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 secure-user authentication protocol considering the mobility based on IPv6 in a wireless LAN environment. Furthermore, we propose a mechanism to enhance wireless LAN security-protection related information, 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 the APs above, we conform that the proposed protocol can be made secure from various attacks and provide convenient and real-time user authentication.

Keywords: WLAN, 802.11f, authentication protocol, security

1 Introduction

Through the Access Point (AP) connecting a WLAN and Local Area Network (LAN), a mobile device employing a wireless network interface card can access the information from the system connected by the LAN. Compared with other mobile communication techniques, the WLAN technique can provide higher performance with lower cost, and can be used widely in wireless internet commerce services. Like cable networks, WLAN needs some access control to be permitted in order to use the information system in the LAN. Also, preventing the combined WLAN and LAN from possible eavesdropping by the tools like sniffers is required. Thus, a secure user authentication protocol needs to be developed for the WLAN environment.
Wireless LAN (WLAN) refers to the wireless network environment constructed indoors or outdoors, by using either radio or light wave technology instead of wire signals from the hub to such clients as PCs (Personal Computers), notebook PCs and PDAs. TGf (Task Group F), among IEEE 802.11 WGs (Working Groups) has proposed IAPP (the 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.

We propose a mechanism to enhance the wireless LAN security user authentication protocol considering the mobility based on IPv6 in a wireless LAN environment. Furthermore, we propose a mechanism to enhance the wireless LAN security protection related information, 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, we confirm that the proposed protocol can be secure from various attacks and provide convenient and real-time user authentication.

The organization of the paper is as follows. Section II presents related works. In Section III, we propose a user authentication protocol mechanism. The implementation and Security Evaluation of the proposed security mechanisms is presented in Section IV. Finally Section V concludes the paper.

2 Related Work

2.1 EAP (Extensible Authentication Protocol)

EAP is a method of conducting an authentication conversation between a supplicant and an authentication server [1]. It is also an authentication protocol for a general purpose. The authentication methods in EAP include message digest 5 (MD5), transport layer security (TLS), tunneled TLS (TTLS), and so on. These method protocols have features as follows:

* EAP-MD5 [2]: EAP-MD5 uses challenge handshake authentication protocol (CHAP [3]) which is a challenge-response process for the user authentication portion. It is one of the most popular EAP types because it is easy to use. The authentication server asks for the password by sending a RADIUS-Access-Challenge. The password hash is then sent by using an EAP-Response, which is further encapsulated by a RADIUS-Access-Request.

* EAP-TLS [4]: EAP-TLS provides a way to use certificates for both the supplicant and the server to authenticate each other. Therefore, the forged APs can be detected. Both the supplicant and the authentication server need to have valid certificates when using EAPTLS.
* EAP-TTLS [5]: EAP-TTLS extends EAP-TLS to exchange additional information between the supplicant and the authentication server by using the secure tunnel established by TLS negotiation. An EAP-TTLS negotiation comprises two phases: the TLS handshake phase and the TLS tunnel phase. During phase one, the TLS process is used for the supplicant to authenticate the authentication server by using certificates. In phase two, the authentication of the supplicant can use any non-EAP protocols [6].

![Diagram of EAP-based authentication procedure flow](image)

**Fig. 1.** EAP-based authentication procedure flow

### 2.2 IEEE 802.1x

The IEEE 802.1x standard specifies how to implement port based access control for IEEE 802 LANs, including a wireless LAN [7]. In IEEE 802.1x, the port represents the association between a WLAN station and an AP. Basically, the IEEE 802.1x has three entities which are a supplicant, an authenticator, and a backend authentication server. In the context of a wireless LAN, the supplicant is a wireless LAN station, the authenticator is an AP, and the authentication server can be a centralized remote access dial-in user service (RADIUS) server.

The authenticator controls the authorized state of its controlled port depending on the outcome of the authentication processes. Before the supplicant is authenticated, the authenticator uses an uncontrolled port to communicate with the supplicant. The authenticator blocks all traffic except the EAP messages before the supplicant is authenticated. IEEE 802.1x employs EAP as an authentication framework that can carry many authentication protocols, between the supplicant and the authenticator [8] [9]. The protocol between the authenticator and the authentication server is not specified in the IEEE 802.1x standard. Instead, IEEE 802.1x provides RADIUS usage guidelines in the Annex.
2.3 IEEE 802.11i

IEEE 802.11i provides enhanced security in the medium access control (MAC) layer for IEEE 802.11 networks [10] [11]. One of the major missions of IEEE 802.11i is to define a robust security network (RSN). The definition of an RSN according to IEEE 802.11i specification is a security network that only allows the creation of robust security network associations. To provide associations in an RSN, IEEE 802.11i defines authentication, encryption improvements, key management, and key establishment. As shown in Fig. 2, in the first stage, IEEE 802.11i starts with Open System Authentication defined IEEE 802.11. And the WLAN station is authenticated and associated with an AP. At the end of this stage, IEEE 802.1x port remains blocked and no data packets can be exchanged. The second stage consists of IEEE 802.1x authentication which employs extensible authentication protocol (EAP) to authenticate users. A user can surf the Internet after the completion of 4-Way Handshake execution in the third stage.

2.4 IAPP (Inter Access Point Protocol)

2.4.1 IAPP Structure

IAPP is initialized while exchanging IAPP-INITIATE service primitives 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 [12] when it receives an 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 a 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

2.4.2 IAPP Mechanism Overview

IAPP is a protocol that is designed to ensure mobility among APs on a sub-network. It provides 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, a distribution system, and one or more RADIUS servers. It uses ESP as the security algorithm to relay WEP keys between two APs. It gets the 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 Fig. 3 STA requests AP2 for reset when it enters the latter’s domain. If AP2 uses Proactive Caching [13], APME first searches the terminal’s context data in the IAPP cache using the terminal’s MAC address. When it finds a piece of 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 Fig. 3, the 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 have been 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. 3. IAPP Operation Process
3 A Proposed Protocol for User Authentication

In our proposed user authentication protocol, the user information from a Client is transmitted to the AP through the WLAN, and it is matched with the enrolled-user information at the AS through the LAN. According to the possible attack points in the authentication system, security attacks can be classified into a system module attack, network attack, and database attack [14]. In this paper, we consider only the network attack in the communication channel. The solutions for other types of attacks can be found in [15] [16].

<table>
<thead>
<tr>
<th>Term</th>
<th>Explanation</th>
<th>Term</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Client</td>
<td>AS</td>
<td>Authentication Server</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
<td>KUx</td>
<td>Public Key of x</td>
</tr>
<tr>
<td>IDc</td>
<td>Client ID(Device Identifier)</td>
<td>KRx</td>
<td>Private Key of x</td>
</tr>
<tr>
<td>f(x)</td>
<td>Function for exchange Random Value</td>
<td>AP1</td>
<td>Access Point(Old AP)</td>
</tr>
<tr>
<td>BSSID1</td>
<td>AP1 MAC address</td>
<td>AP2</td>
<td>Access Point(New AP)</td>
</tr>
<tr>
<td>Kap-s</td>
<td>Session Key of Between AP1 and Ap2</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

The details of the hand-off protocol among C, AP1, AP2, and AS (shown in Fig. 4, and Fig. 5) are as follows:

![Fig. 4. Illustration of the user authentication environment](image-url)
Fig. 5. Illustration of the authentication protocol considering the mobility

1) Re-association Request
   ① C -> AP2: EKUc(IDc | BSSID1)

   ② AP2 -> AS: EKUc(IDc | BSSID1)
   When C gets out of the AP1 service area, it performs re-association with AP2. At this time, AP2 forwards the re-association message IDc and BSSID1 encrypted with KUc from C to AS. We use the SSH (Secure Shell) [17] tunnel from the WLAN link.

2) Re-association Reply
   ③ AS -> AP2: EKUap2(ipaddr1 | KUap1 | KUc)
   By decrypting the message 1, AS gets the re-association message received from C. Then, AS gives the re-association information to AP2 for the re-association between AP1 and AP2. In the re-association information, ipaddr1 means the IP address of AP1 to connect AP2 to AP1, KUap1 and KUc are for transmitting the re-association messages from AP2 to AP1 and C, respectively. This re-association information is encrypted with KUap2, and transmitted to AP2.

3) User Authentication Status Challenge
   ④ AP2 -> AP1: EKUap1(Kap-s | Authenticator)
   By decrypting the message 3 with KRap2, AP2 obtains KUc and KUap1. AP2 generates the session key Kap-s sharing between AP1 and AP2, and transmits it to AP1. Consequently, AP1 does not need to request the public key of AP2 to AS. By
applying the one-way hash function to Kap-s, AP2 generates the message authenticator (Authenticator) for integrity. Then, Kap-s and Authenticator are encrypted with KUap1, and transmitted to AP1.

4) User Authentication Status Response

⑤ AP1 -> AP2: EKUap-s(time stamp, authentication status | information)

By decrypting the message 4 with KRap1, AP1 gets the authentication status request of AP2, verifies the Authenticator, and obtains Kap-s. Therefore, AP1 identifies the authentication status of C, and transmits it to AP2. At this time, time stamp is padded into the authentication status message to prevent the replay attack.

5) User Authentication Reply

⑥ AP2 -> C: EKUc(result)

By decrypting message 5 received from AP1 with Kap-s, AP2 obtains the authentication status of C. If the authentication status of C is valid, AP2 transmits the reconnection message to C by encrypting it with KUc. Finally, C can get the reconnection result from message 6.

4 Implementation and Security Evaluation

We present the implementation details and analyze the security of the proposed protocol.

4.1 Implementation Details

The user terminal device and the authentication server are implemented on the Windows XP system. The security module (denoted as Security), the network packet sending and receiving module (denoted as Network Com.), and the protocol processing module (denoted as Protocol Analyzer) are common to both the user terminal device and the authentication server. There is the matching module (denoted as Matcher) in the authentication server.

Both the AP1 and the AP2 are implemented on the ubuntu 6.0 system. There is the mini-shell module to setup the default setting in the AP. We used MD5 [18], RSA [19] as hash function, symmetric encryption, and asymmetric encryption, respectively.
Fig. 6 shows the prototype of our authentication system. The authentication system consists of: ① user client, ② AP1(Access Point 1), ③ AP2(Access Point 2), ④ AS(Authentication Server). In this system, ① is connected to the WLAN, and ②, ③, ④ are connected to the LAN. ②, ③ serve as the bridge between WLAN and LAN.

4.2 Security of the Proposed Protocol

Denial of Service and Rogue Station Attack

A DoS (Denial of Service) attack is a malicious attempt by a single person or a group of people to cause the victim, site, or node to deny service to its customers. When this attempt derives from a single host of the network, it constitutes a DoS attack. On the other hand, it is also possible that a lot of malicious hosts coordinate to flood the victim with an abundance of attack packets, so that the attack takes place simultaneously from multiple points. This type of attack is called a Distributed DoS, or DDoS attack, exactly an attacker overloads an AP in various ways so that the AP is unable to serve legitimate users. The attacker does not directly benefit but creates a nuisance, and rogue station attack is a rogue station affinitizing itself with an AP. The attacker benefits by becoming a participant in the wireless network and thus gaining the ability to send and receive data.

In our authentication protocol, additional parameters (i.e., old authentication status and authentication information) are padded into challenge response messages, thus protecting from denial-of-service attacks and rogue station attacks.

Denning-Sacco (DS) Attack Prevention

Although an attacker can obtain the session key, it cannot be reused in the next authentication session. It is because the protocol uses the time information time stamp
as well as the random numbers f(ipaddr1). Therefore, probability which an attacker can reuse the authenticated user information decreases slightly.

**Replay Attack Prevention**

By using the replay attack, an attacker could pretend to be an authorized user to access a network. For example, an attacker could simply intercept and replay a station's identity and password hash to be authenticated.

In general, an attacker can perform a replay attack in the WLAN/LAN. To solve this attack, we considered several steps. First, From AP2 to AP1 messages transmitted from each node always include pseudorandom numbers f(ipaddr1). Second, by applying the one-way hash function, the receiver can verify the integrity of the transmitted message. Thus, for all communication channels, the end-to-end security for protecting the authentication status, time stamp and information can be guaranteed.

**5 Conclusion**

In this paper, we have proposed a mechanism to enhance the wireless LAN security user authentication protocol considering the mobility based on IPv6 in a wireless LAN environment. Furthermore, we have proposed a mechanism to enhance the wireless LAN security protection related information, 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, and thus we confirm that the proposed protocol can be secure from various attacks and provide convenient and real-time user authentication.

Based on the WLAN-based implementation, we believe the proposed protocol can be used for secure and convenient user authentication. Note that the proposed protocol can also be applied to other biometrics information, such as speaker verification [20]. In the future, we would extend our protocol using Mobile IP and consider the packet loss problem during the handoff.

**6 Acknowledgements**

This research was financially supported by the Ministry of Commerce, Industry and Energy (MOCIE) and Korea Industrial Technology Foundation (KOTEF) through the Human Resource Training Project for Regional Innovation.
References