Designs of a Secure Wireless LAN Access Technique and an Intrusion Detection System for Home Network

Tae-Sub Kim¹, Yi-Kang Kim¹, Byung-Bog Lee², Seung-Wan Ryu², Choong-Ho Cho¹
¹Department of Computer and Information Science, Korea University
²Department of Information Systems, Chung-Ang University, Korea
³Electronics and Telecommunications Research Institute
{ree31206, kimyikang, chcho}@korea.ac.kr, rush2384@cau.ac.kr, bblee40@etri.re.kr

Abstract

IEEE 802.11i standard supports a secure access control for wireless LAN and IEEE 802.1x standard includes various authentication method protocols. It is expected that next generation wireless LAN security techniques will be based on IEEE 802.1x and IEEE 802.11i standards. However, at present users who are not familiar with a computer and an authentication details have difficulty to setup the network security based on IEEE 802.11i. Accordingly, this paper proposes authentication scenarios to minimize the process needed by users, a password method which is changed randomly and periodically, and authentication protocols. The proposed protocols provide convenience for nonprofessional computer users as well as secure the home network environment against the unwanted attacks such as a dictionary attack or a replay attack and it uses SNMP and the system to be able to detect an intrusion it supposes will occur.

1. Introduction

Home network service has been integrated with various communication technologies to help people have a more convenient life. It is expected that wireless LAN (WLAN), Bluetooth, ultra wide band (UWB), and Zigbee will be used in home networks as wireless access technologies to provide various home network services. WLAN study among them is actively making progress. But WLAN communication technologies have a problem in that access points (APs) cannot control the transmission range. This property allows the neighbor or person in the next house to receive the traffic and a malicious intruder to subvert the privacy. Therefore, authentication mechanisms have to be considered so that only an eligible user is authenticated to use the resources of a home network.

IEEE 802.11i working group (WG) specifies an authentication procedure but it provide the only basic mechanism which can not protect the WLAN communications from the ineligible approach. The IEEE 802.11i standardization group is working on an access control based on IEEE 802.1x and air traffic encryption to strengthen WLAN security techniques. In a conventional method, the nonprofessional user finds it very difficult to setup security information inside WLAN stations and APs. However, there are the various user levels of computer knowledge in a home network. Because of this reason the easy way to setup authentication information should be prepared so it is easy for users who are not computer professionals [1].

In this paper, we propose access control mechanism considering the convenience of users, secure authentication protocol, and the intrusion detection system to support access control mechanism. Section II presents related works. In Section III, we propose authentication mechanism and the intrusion detection system for home network. The performance analysis 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 [2]. It is also an authentication protocol for 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** [3]: EAP-MD5 uses challenge handshake authentication protocol (CHAP [4]) 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 RADIUS-Access-Challenge. The password hash is then sent by using EAP-Response, which is further encapsulated by RADIUS-Access-Request.

* **EAP-TLS** [5]: 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 EAP-TLS.

* **EAP-TTLS** [6]: 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 [7].

To apply these protocols mentioned above to the user’s device, the user has to know how to setup these authentication protocols. Accordingly, it needs a simple and easy way to authenticate the home network users. In this paper, we consider the home network user who is not familiar with the authentication method. We also discuss how to provide automatic authentication mechanism for the users.

IEEE 802.1x standard specifies how to implement port based access control for IEEE 802 LANs, including wireless LAN [8]. In IEEE 802.1x, the port represents the association between a WLAN station and an AP. Basically 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 [5], [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.

**Fig. 2. IEEE 802.11i-based authentication procedure flow**

**2.3. IEEE 802.11i**

IEEE 802.11i provides enhanced security in the medium access control (MAC) layer for IEEE 802.11 networks [1], [10]. 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 Figure 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. SNMP (Simple Network Management Protocol)

The SNMP is a management protocol used to manage TCP/IP networks. Nowadays, it is widely used in several commercial networks, since it is a relatively simple protocol, but powerful enough to be used in the management of heterogeneous networks. The SNMP management comprises an agent, a manager and a MIB (Management Information Base), as shown in Figure 3. The MIB is a database composed of objects that will be managed and/or monitored through the SNMP protocol. A manageable object represents a real resource in the network, such as a rotator, a switch and also the final system resources, like, for example, CPU, memory, etc. Each manageable object has a set of variables of which values can be read or altered by the agents.

![Fig. 3. Relation between components of the SNMP Management](image)

3. Design of the Security Home Gateway Server

A security home gateway server is proposed to guard the access to the network [5]. The security home gateway server collects and processes security related information from managed devices. It acts as the entry security provider for guarding the proper usage of upper layer application services, such as alarm reporting. Among these network management applications, both type of alarm reporting are of interest in this paper. As shown in Figure 4, this security home gateway server consists of five management units: traffic collection unit, traffic processing unit, authentication unit, policy management unit, and response unit. The gateway also cooperates with an authentication server to guarantee a secure link layer access control. Also to protect intrusion detection the AP must support SNMP agent functions and the security home gateway sever must support SNMP server functions.

![Fig. 4. Security home gateway system server architecture](image)

**Traffic Collection Unit:** The unit collects traffic from routers, access points among other devices. The communication information can be obtained by log files, traffic mirror, or by polling SNMP agents on managed devices. The gathered information is passed to traffic processing unit for further classification and computation.

**Traffic Processing Unit:** This unit processes the data from the traffic collection unit. For example, Data packages are classified according to the type of ICMP, TCP, UDP, SNMP and others, such as IP source and destination addresses. All data are stored in the database associated with timestamps.

**Authentication Unit:** This unit works together with APs. It is responsible for a port-base access control protocol, as specified in 802.1x. The authentication request, issued by a wireless client, is passed, by AP’s forwarding feature, to the RADIUS server for verification. Using the information replied from the RADIUS server, access policy of the requesting client can be determined at AP. The authentication results are passed to behavior analysis unit for further processing.

**Policy Management Unit:** According to the vulnerabilities and threats we described in last section, there exist certain patterns for each potential security flaw. The characteristics of each attack or abnormal behavior are analyzed and predefined as security policies. Depending upon the management requirement, a policy could also be updated by security configuration management.
Response Unit: The response unit is responsible for notifying the network management server an abnormal behavior or for updating security configuration. Management applications of alarm reporting react upon receiving the messages from response unit correspondingly.

All five management units are integrated together to provide precaution security application services. Specifically, by cooperating with an authentication server, access control in the link layer is provided; by monitoring and analyzing data packages, the security threats prevention can be achieved in IP layer.

3.1. The Proposed Protocol

To support the mentioned scenarios, the authentication protocol requires additional message exchanges including information which is not specified in Standards. Periodic changes may be problems from the viewpoint of users, when the password is changed while a user takes the WLAN station out of home. The WLAN station needs to be authenticated again when the user brings the WLAN station back to home. However the WLAN station can not obtain the authority without user's assistance since the password is already changed. Other devices in home network also are needed to know the new password to keep the authority.

Table 1. The MAC Address Management Table

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Authentication number</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:F0:7A:B1:B7</td>
<td>1</td>
</tr>
<tr>
<td>00:00:F1:7A:B4:77</td>
<td>2</td>
</tr>
<tr>
<td>00:00:F1:8A:BB:A7</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 2. The Authentication Number Management Table

<table>
<thead>
<tr>
<th>Authentication Number</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1234</td>
</tr>
<tr>
<td>2</td>
<td>5678</td>
</tr>
<tr>
<td>3</td>
<td>9123</td>
</tr>
</tbody>
</table>

The proposed protocol solves the problem by adding the authentication number. The authentication number is an index number which corresponds to each password. It is numbered randomly whenever the password is changed. The security home gateway server manages two tables. One is the MAC address management table which records the MAC addresses of the authenticated devices and the authentication number. The other is the authentication number table. When the password is changed, the password and the authentication number are recorded in the authentication table. For example, there is a device which has the MAC address of 00:00:F0:7A:81:B7. After the device is authenticated when the password is 1234, the server records its MAC address with the current authentication number in the MAC address management table as shown in Table 1. Then the server transmits the current authentication number to the device. In this case, the current authentication number is 1. When the password is changed to 5678, as shown in Table 2, the authentication number is also changed to 2 and recorded in the authentication number table.

Figure 5 presents the EAP-TTLS procedure to support the proposed authentication protocol. In this figure, the solid lines represent legitimate message exchanges and the dashed lines indicate supplementary message exchanges. As shown in Figure 6, the EAP-TTLS procedure by using the authentication number is as follows.

1. The user's WLAN station associates with an AP using open authentication with wired equivalent privacy (WEP) turned off. Then the AP asks for the user's identity.
2. The WLAN station transmits an EAP-request message encapsulated in an EAPoL-EAP frame to the AP, which contains the MAC address of the WLAN station.
3. The server is authenticated to the WLAN station using its security certificate and a TLS connection is established between them. The encryption key for the TLS connection will be used for air traffic encryption.
4. Inside the TLS connection (inside box), the exchanged messages are encapsulated into TLS records that are again encapsulated into EAP-request and EAP-response messages. In the existing protocol, the WLAN station informs the AP of a user name and a password. In addition, we propose that the WLAN station sends both the old authentication number and authentication status in the same EAP-Response message. After receiving it, the AP relays it to the server.
5. The server then verifies the old authentication number to determine whether the MAC address and the old authentication number of the WLAN station are the same as the stored data in the MAC address management table.
6. After the old authentication number is authenticated by the WLAN station, the server transmits the new authentication number to the WLAN station through the AP. The WLAN station which received the new authentication number information updates the authentication information for itself. The
server will complete the course of authentication by using the password corresponding to the authentication number table. At this point, the authentication method is able to use many protocol. Here, we assume that CHAP is used.

7. The EAP-TTL procedure ends by sending the EAP success message to the WLAN station.

In this paper, we use the EAP-TTLS protocol since the user name, password and authentication information are protected by the TLS connection. The proposed protocol also can be applied to EAP-MD5, EAP-TLS and other protocols. To inform the new authentication number from the server to the WLAN station, the server sends its authentication number and MAC address together with identity.

The server sends the message that contains authentication information and updates the table. However there is a risk of man-in-the-middle attacks by which the current password and authentication information can be stolen. Hence we suggest that the transmitted information is encrypted by the password like TTLS protocol.

![Diagram](image)

**Fig. 5.** The proposed protocol flow

### 3.2. Packet Format

The format of EAP packet is shown in Figure 6. (a) is the EAP packet format, (b) is the EAP-TLS packet format, and (c) is the proposed packet format.

(a) EAP packet format

<table>
<thead>
<tr>
<th>Code</th>
<th>Identifier</th>
<th>Length</th>
<th>Type</th>
<th>L</th>
<th>M</th>
<th>S</th>
<th>R</th>
<th>V</th>
<th>TLS message length</th>
<th>TLS Data</th>
</tr>
</thead>
</table>

(b) EAP-TLS packet format

<table>
<thead>
<tr>
<th>Code</th>
<th>Identifier</th>
<th>Length</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>S</td>
<td>A</td>
<td>V</td>
</tr>
</tbody>
</table>

| Byte | Byte | Byte | Byte | Byte |

(C) The proposed packet format

**Fig. 6.** Packet format

Code is one byte indicating the type of packet; 1 indicates Request, 2 indicates Response, 3 indicates Success and 4 indicates Failure. Identifier is a value in the range 0-255 and it should be incremented for each message transmission. This helps to check which Response goes with which Request. Length is the total number of bytes in the EAP message. The Type field indicates the type of Request or Response. For example, 1 means the identity packet and 13 means the EAP-TLS packet. The Data field is the actual request or response data being sent. The format of the data field is determined by the Code field. If the Code field is 3 or 4 that is a success or a failure, these messages contain no data. In case of EAP-TLS, Data field is divided into more parts as shown in Figure 6 (b). L, M, S, R, and V are flags which mean the length included, more fragments, start flag, Reserved, and Version number respectively.

For the backward compatibility, the proposed protocol uses the same packet format. In case of the EAP-TTLS protocol, we can use the existing packet format because the packet format for new messages and the additional information is able to use the same format as other messages. We change only the reserved bit with the C bit that means the authentication number is included. If the C bit is set in the EAP message, it means that the message includes the authentication number or the authentication information. But when EAP-MD5 or EAP-TLS is used, the authentication number is added to identity message. The authentication server cannot separate the authentication number from the user's identity. Therefore, it needs a new type instead of 1 which means the identity. It can be other number for the Type field. In addition, the Data field can be divided...
into two parts: the former part is used for the authentication number and the latter part is used for the identity. Additional messages that carry the authentication information are used in the same packet format as EAP-TTLS.

3.3. The Proposed Intrusion Detection System

In the proposed intrusion-detection system, the secure home-gateway server (i.e., SNMP server) identifies whether or not the terminal node is an authenticated MAC address by polling (See Figure 1). If this MAC address is violated, an alarm message notifies the response unit inside the home. This solves some leakage. Now the user should enroll the MAC address of the AP. Additionally, SNMP can obtain some traffic information (i.e., ICMP, TCP and UDP, etc.). If this traffic quantity is increased beyond a specific threshold, the user may consider it an intentional/unintentional leakage (i.e., an attack of intentional connection or DoS attack). Thus, the response unit warns of the leakage inside the home by giving an alarm message.

4. Security Analysis

EAP-MD5 is more vulnerable to unwanted attacks than other authentication methods. One of such attacks is a brute force attack. A brute force attack is a method of defeating a cryptographic scheme by trying a large number of possibilities, for example, exhaustively working through all possible keys in order to decrypt a message. To protect the brute force attack, at least, the password should be changed by every month. The proposed protocol is robust to the brute force attack since it changes the password periodically.

It also helps to detect a replay attack. 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. When a user doesn't use the authentication number, a hacker can receive the challenge message and transmit the response message repeatedly. On the contrary, when the authentication number is used, a hacker also should know it. It is easy to know user's identity. But it is not easy to know the authentication number because it is transmitted under encryption in the previous authentication procedure. Therefore, the server can detect a hacker who uses the authentication number invalid. In our authentication protocol, additional parameters (i.e., old authentication number and authentication status) are padded into challenge response messages, thus protecting from replay attack.

4.1. Password Dictionary Attack

A method used to break security systems, specifically password based security systems, in which the attacker systematically tests all possible passwords beginning with words that have a higher possibility of being used, such as names and places. The word dictionary refers to the attacker exhausting all of the words in a dictionary in an attempt to discover the password.

This paper proposes authentication scenarios to minimize the process needed by users, a password method which is changed randomly and periodically, and authentication protocols. Also because it added a new parameter, being safe consequently, more it will be able to provide the home network environment which is convenient.

4.2. Replay Attack

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. When a user doesn't use the authentication number, a hacker can receive the challenge message and transmit the response message repeatedly. On the contrary, when the authentication number is used, a hacker also should know it. It is easy to know user's identity. But it is not easy to know the authentication number because it is transmitted under encryption in the previous authentication procedure. Therefore, the server can detect a hacker who uses the authentication number invalid. In our authentication protocol, additional parameters (i.e., old authentication number and authentication status) are padded into challenge response messages, thus protecting from replay attack.

4.3. Denial of Service and Rogue 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 number and authentication status) are padded into challenge response messages, thus protecting from denial of service attack and rogue station attack. Also, this proposed intrusion detection system, if this MAC address is violated, alarm message is notified to response unit inside home. This solves some leakage that user should enroll MAC address of AP. Additionally, SNMP can obtain some traffic information (i.e., ICMP, TCP and UDP etc). If this traffic quantity is increased more than specific threshold, user may consider an intentional/unintentional leakage (i.e., an attack of intentional connection or DoS attack). Thus, response unit alarms the leakage inside home by alarm message.

5. Conclusion

We introduced secure and convenient mechanisms for home network WLAN access. We also proposed the authentication protocol to provide the automatic authentication when the password is changed. The automatic-password change method enables users to use the home network without periodic password changes. Under the threats we considered, the proposed protocol appeared to give a protection against a dictionary attack, a replay attack, a denial of service attack and a rogue station attack. Although the password used before is changed for some reasons, the users do not need to enter the new password or other information again. From the viewpoint of users, the mechanisms applied in the proposed protocol are convenient since users do not need to know the authentication mechanism. Also, it used the SNMP protocol so that the inside home user will be able to perceive an attack.

For the backward compatibility between the authentication methods, we modified the packet format using a reserved bit. The C bit is added for the authentication number and the new type number which indicates not only the user’s identity but also the authentication number should be used.

Compared with the current security set up procedure for WLAN, the proposed protocol can provide a simple procedure for WLAN users and protect them from unwanted attacks in home network environment.

6. Acknowledgements

This research was supported by the MOCIE (Ministry of Commerce, Industry and Energy), Korea, under the growth engine technological development program supervised by the ITEP (Korea Institute of Industrial Technology Evaluation & Planning).

7. References