# Denial of Service Attack against IEEE 802.11 WLAN Fast Initial Link Setup Technology

Sokjoon Lee, and Byung Ho Chung

***Abstract*—**Many users are using IEEE 802.11 WLAN technology for accessing Internet in hotspot and enterprise environments. However, in spite of progress of network throughput, the users sometimes feel inconvenience about the long initial access time for secure authentication, link layer key exchange and IP address setup. In order to solve this problem, IEEE 802.11ai adopts the fast initial link setup (FILS) with EAP reauthentication protocol (ERP). With FILS, the initial access time including authentication can be reduced when user connect a wireless network again after the first connection and authentication.

Meanwhile, there are security threats in IEEE 802.11 WLAN technology such as eavesdropping, rogue access point attack, denial of service, etc. Especially, denial of service attack is possible using the essential flaw of IEEE 802.11 or 802.1X protocol. Similarly, this type of attack is also possible in FILS process. In this paper, we introduce three examples of denial of service attacks in FILS and propose the countermeasure against these attacks.

***Keywords*—**Denial of service attack, FILS, IEEE 802.11ai

## I. Introduction

IEEE 802.11 based wireless LAN technology is standardized for supporting wireless local area communication using 2.4GHz and 5GHz RF bands. Since the first version was released in 1997, the additional requirements have been adopted in the subsequent amendments such as fast speed, Quality of Service (QoS), security, etc. As Internet access using wireless LAN is becoming common, the users have more possibilities to encounter attacks exploiting the vulnerabilities of the network. These kinds of attacks include eavesdropping, rogue access point and denial of service using packet forgery.

Recently, there are many discussions about reducing initial access time in IEEE 802.11ai task group [1]. These discussions focus on two points; the fast network discovery and concurrent higher layer setup. The second one of concurrent higher layer setup is discussed for reducing the number of packets used in authentication and IP address setup processes. The fast initial link setup (FILS) with EAP reauthentication protocol (ERP) [3] is adopted instead of EAP protocol [2] used IEEE 802.1X.

Therefore, this technology can make the user authentication faster than the conventional authentication protocol like PEAP. Moreover, the ERP packets between the clients and access points are exchanged over IEEE 802.11 authentication and association request/response frames and this process also reduces the total number of the exchanged frames.

However, packet forgery is very easy in IEEE 802.11 WLAN and denial of service attacks is possible with this vulnerability. This situation may not be different in FILS process. If the attacker counterfeits the authentication and/or association frames, ERP protocol will not work well and the WLAN users can be in trouble to access Internet. In this paper, we introduce three examples of denial of service attacks in FILS and propose the countermeasure against these attacks.

## II. Background

### A. IEEE 802.11ai Fast Initial Link Setup (FILS)

For subscriber management and data privacy, WLAN service providers generally use IEEE 802.1X based user authentication and WPA (or IEEE 802.11i) based link layer data security technologies in enterprise or hotspot environment. After authentication, the subscriber devices get IP addresses dynamically using DHCP because they do not access the network in the fixed location. Though these processes provide the enhanced security and convenient mobility, they have disadvantage of long access time.

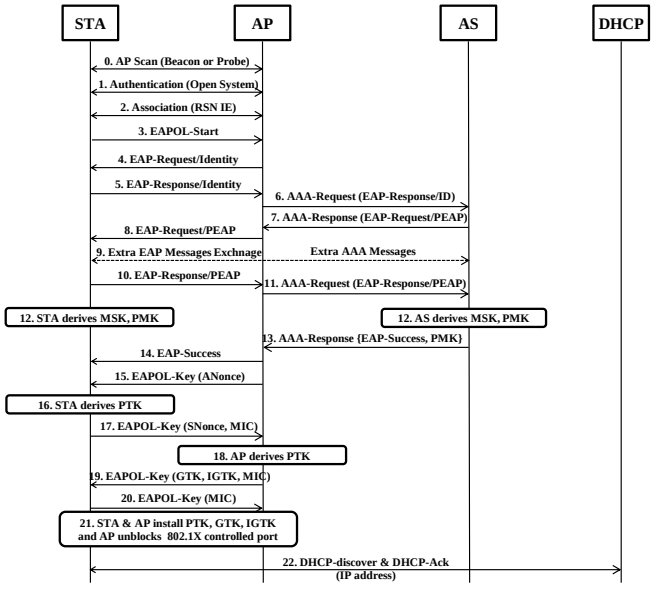


Fig. 1 IEEE 802.11-based Original Setup Process

Sokjoon Lee is with Electronics and Telecommunication Research Institute, Daejeon, South Korea (corresponding author to provide phone: +82-42-860-5455; fax: +82-42-860-1471; e-mail: junny@etri.re.kr).

Byung Ho Chung is also with Electronics and Telecommunication Research Institute, Daejeon, South Korea (e-mail: cbh@etri.re.kr).

Fig. 1 shows IEEE 802.11-based original setup process using IEEE 802.1X-based user authentication and WPA-based link layer data security. In this figure, there are very many packets exchanged between the device and access points. The packets for IEEE 802.11 authentication/association, EAP, EAPOL 4-way handshake and DHCP are exchanged separately. If there is a method that these packets are reduced to a few packets by combining some packets, it is possible to reduce the setup time.

IEEE 802.11ai task group focuses on this problem to enable fast initial link setup. The group adopts fast initial link setup (FILS) to reduce initial association time to allow fast connection and data transfer in situations where users are very dense and highly mobile.

First, the group use EAP reauthentication protocol (ERP) to reduce authentication packets themselves after the user is authenticated using EAP. In most EAP methods such as PEAP, the device and access point should send very many packets for authentication. But, ERP requires only 4 packets if they once established the successful authentication using EAP. Second, they combine IEEE 802.11 authentication /association, ERP, EAPOL 4-way handshake and DHCP to only 4 packets.

The task group approved draft standard version 1.0 in August, 2013 and the version 6.0 is published in July 2015. As the modified setup, FILS makes the user authentication and key exchange faster than the original setup. The total FILS process is shown in Fig. 2.

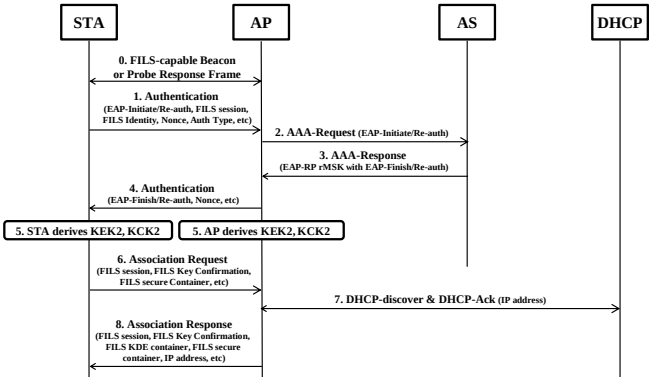


Fig. 2 IEEE 802.11ai Fast Initial Link Setup Process

In Fig. 2, IEEE 802.11ai FILS uses ERP instead of EAP. ERP packet for user authentication and key exchange for link layer is delivered in IEEE 802.11 authentication frame. In order to generate secure session key using master session key (MSK) which was shared between device and authentication server, at least three-way handshake should be established. Considering this, nonce value is exchanged in IEEE 802.11 authentication frame. Other information for establishing secure session key is also delivered over IEEE 802.11 association frame. This mechanism is similar with WPA 4-way handshake.

### *B. Denial of service attacks in IEEE 802.11 WLAN*

As mentioned in Section 1, packet forgery is very easy in IEEE 802.11 WLAN. Aircrack-ng [7] or other tools can be used for this with ath9k driver with Atheros WLAN network interface card (NIC) in linux and Airpcap-nx USB WLAN NIC [8] in Microsoft Windows.

One example of the attacks using packet forgery is deauthentication flooding attack. IEEE 802.11 deauthentication frame is one of the management frames and can be sent by device or access point in order to terminate the current communication. Therefore, if an attack forges the deauthentication packet, of which source is access point A and the destination is device B, the device B will terminate the connection with the access point. If the attacker generates the forged deauthentication frame continuously, the device will not be able to connect to the access point. This type of attack is called deauthentication denial of service or deauthentication flooding attack.

There are various types of denial of service attacks in IEEE 802.11 WLAN environments. Some attacks can terminate the current connection, while other attacks make the resource of access point exhausted such as association flooding attack.

## III. Denial of Service in FILS

In this paper, we introduce three types of denial of service attacks, which make FILS work improperly; ERP failure attack, ERP authentication flooding attack and FILS handshake corruption attack.

### *A. ERP Failure Attack*

In Fig. 2, there are 4 messages exchanged between device and access point except the scanning message of beacon or probe. The first 2 authentication frames contains ERP packets, which recycle the old session key established from the previous EAP authentication session. If the device and authentication server have the same old session key (EMSK in EAP), they succeed in authenticating each other again in the ERP session.

In successful ERP session, they can derive rRK (reauthentication Root Key) and the authentication server sends EAP-Finish/Re-auth packet with setting R-bit as 0 to the device through access point. There will be a little delay in FILS, compared with the original IEEE 802.11 protocol, because the first ERP packet should be delivered to the server, the server should process the EAP-Initiate/Re-auth, etc.

An attacker can abuse this delay. If the attacker monitors the channel used by an access point, it will be able to see the authentication frame for FILS. Then, at the moment that the attacker receives any authentication frame for FILS from any device, the attacker can forge the corresponding authentication frame from the access point. The forged frame will include EAP-Finish/Re-auth packet with setting R-bit as 1. The device will receive the forged frame prior to the normal frame, because the normal frame has a little delay to arrive to the device.

When the forged frame is received, the device will regard the FILS process as failure and it will try to start the original 802.1X authentication process. This ERP failure attack is similar with EAP success flooding and EAP failure flooding, which are already known in the previous research [4].

### *B. ERP Authentication Flooding Attack*

The attacker can forge a numerous IEEE 802.11 authentication frames including EAP-Initiate/Re-auth packet which have different source addresses. In this case, the access point deems that there are a numerous devices which want to access the access point. Whenever the access point gets a forged frame, the access point will generate the corresponding RADIUS message including the ERP packet and send it to the authentication server.

If the attacker takes NAI information in advance which is authenticated using EAP and can be reauthenticated and use the information in the forged frames, the server should find the original session key from database using the NAI, compute rRK and send the response to the access point whenever the forged ERP packets are received. It will waste a lot of resource in the authentication server.

Also, the access point should regard all forged (virtual) devices as real ones and allocate the resource for the authentication session. If all resources are allocated, the access point cannot work well or the normal device cannot connect the access point.

This attack is similar with authentication flooding or association request flooding attacks [4], but the different is that this attack influences the authentication server while the latter one does not.

### *C. FILS Handshake Corruption Attack*

When association request and response frames are exchanged between device and access point, the frames include FILS Key Confirmation data. This is similar with EAPOL 4-way handshake in the conventional IEEE 802.11i or WPA. If the device and the authentication server have the same rRK and the rMSK derived from the rRK is passed to the access point, then the device and access point can generate the same PMK using FILS Key Confirmation data in this process.

The attacker normally does not have a method to know this PMK. Then the WPA session will be kept secure even if the attacker monitors these association packets. But, by forging these association packets, the attacker can make the device and access point fail to have the same PMK.

If they failed, they should restart the FILS or full EAP authentication and key exchange.

## IV. COUNTERMEASURES

There is no method to make the attacks described in Section III disappear. Therefore, it is very important to detect the attacks and report it to the WLAN operator or manager. Two approaches are possible for this.

First approach is to use WIDS/WIPS [5], [6] to detect the attacks. In this case, the WIDS/WIPS product should include the detection mechanism of these attacks. The monitoring sensors should be deployed in the physical area to detect abnormal WLAN frame. Therefore this product is suitable for the enterprise WLAN environment. However it is not applicable in hotspot environment because hotspot service is provided in unlimited physical area.

The second approach is that access point has the function to detect these attacks. For examples, the access point has the capability to decide if there is the ERP failure attack in the current FILS. If the access point sees the device who want to the normal EAP process even after the access point send the successful EAP-Finish/Re-auth, the access point can doubt the current FILS process.

## V. CONCLUSION

In this paper, we introduce three examples of denial of service attacks in FILS and propose the countermeasure against these attacks. The effects from the first and third attacks are not severe because only the device and access point are influenced. The second attack seems to be severe because the central authentication server can be damaged. However, it is considerable that the packet forgery for the attacks is very easy if the attacks are severe or not. The forgery is very similar with the previous attacks. A just little modification can make FILS work not well.

There is no implementation of these attacks in the real world because there is no WLAN product which applies IEEE 802.11ai. But, if the products supporting IEEE 802.11ai are produced by any vendor, it will be possible to test the attacks and countermeasures.

## ACKNOWLEDGMENT

This research was funded by the MSIP (Ministry of Science, ICT & Future Planning), Korea in the ICT R&D Program 2015 [Development of International Standards Smart Medical Security Platform focused on the Field Considering Life Cycle of Medical Information]

## REFERENCES

[1] IEEE P802.11ai: Draft Standard for Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications-Amendment 7: Fast Initial Link Setup, 2015.

[2] RFC 3748, Extensible Authentication Protocol (EAP), http://tools.ietf.org/search/rfc3748, 2004.

[3] RFC 6696, EAP Extensions for the EAP Re-authentication Protocol (ERP), http://tools.ietf.org/html /rfc6696, 2012

[4] C. He and J. C. Mitchell, "Security Analysis and Improvements for IEEE 802.11i," The 12th annual network and distributed system security symposium (NDSS'05), 2005, pp. 90-110.

[5] AirTight, http://www.airtightnetworks.com/home/products/AirTight-WIPS .html

[6] AirDefense, http://www.motorolasolutions.com/US-EN/Services/Run/Network+Infrastructure+Management/IT/AirDefense_Services_Platform

[7] Aircrack-ng, http://www.aircrack-ng.org/

[8] Riverbed Wireless Traffic Capture – AirPcap Adapter for Microsoft Windows, http://www.riverbed.com/products-solutions/products/performance-management/wireshark-enhancement-products/Wireless-Traffic-Packet-Capture.html