情報保護學會論文誌
第13券 第6號, 2003. 12

무선 LAN에서 Inter-Access Point Protocol을 이용한 안전한 핸드오버

양 대 헌*†‡

Secure Handover Using Inter-Access Point Protocol in Wireless LAN

DaeHun Nyang*†‡

요 약

IEEE 802.11 네트웍에서 핸드오버는 반복되는 인증 및 키교환 절차를 요구하며, 이는 seamless 무선랜 서비스를 제공하는데 있어 큰 방해요소가 된다. 이 논문에서는 IEEE 802.11f를 이용한 빠른 키교환 및 인증 방법을 제안한다. 특히, IEEE 802.11i의 4-way 핸드쉐이크를 표준에 벗어나지 않게 수정하므로써 pre-authentication을 이용했을 때 생길수 있는 perfect forward secrecy문제를 해결한다. 제안하는 방법은 IEEE 802.11f의 context block과 IEEE 802.11i의 핸드쉐이크만을 이용하며, 핸드오버 시에 AAA 서버와의 통신을 요구하지 않으므로써 효율성을 높였다.

ABSTRACT

Handover in IEEE 802.11 requires repeated authentication and key exchange procedures, which are an obstacle to seamless services of wireless LAN. We propose a fast authentication and key exchange mechanism using IEEE 802.11f. Especially, by proposing a modified version of the 4-way handshake of IEEE 802.11i, we solve the perfect forward secrecy problem that arises when the pre-authentication is adopted. The scheme can be implemented only using the Context Block of IEEE 802.11f and the 4-way handshake of IEEE 802.11i without involving authentications server's interaction or non-standard behavior between access points. Our scheme is applicable to devices not supporting the pre-authentication of IEEE 802.11i and also, it can substitute the pre-authentication when the pre-authentication is failed.

keyword : *Wireless LAN, Security, Authentication, Key Exchange, Handover*

Ⅰ. Introduction

Wide prevalence of wireless LAN is accompanied with security problem. Owing to the wireless property of Wireless LAN, it is more vulnerable to passive and active attacks than wire-line LAN.[10] Thus, many efforts have been taken mainly from IEEE standard bodies. Especially, task group I of IEEE 802.11 working group has defined enhanced security functionalities in medium access control layer, which is called RSN (Robust Secure Network).[1] Also, IEEE 802.1x has been established for user authentication and for port based access control.[2] Handover between access points is not common today, but it is getting more popular. However, handover involves security breach, which asks authentication and key exchange procedures to be performed whenever handover occurs. Task group F of IEEE 802.11 is currently developing IAPP (inter-access point protocol) to reduce burden of handover by information exchange between access points, but they have defined only framework for the information

* 인하대학교 정보통신대학원 전임강사(nyang@inha.ac.kr)
† 주저자, ‡ 교신저자, 논문접수일 : 2003년 8월 1일, 심사완료일 : 2003년 11월 13일

exchange.[4] In this paper, we propose a fast authentication scheme during handover using IEEE 802.11f. Also, by modifying the 4-way handshake of IEEE 802.11i, we solve the open problem of perfect forward secrecy during handover in the current IEEE 802.11f and the IEEE 802.11i framework without intervention of RADIUS server.

II. Authentication and Key Exchange in Wireless LAN Framework

Authentication is performed between a station and an authentication server that is normally a RADIUS server through an access point.[7] A station is called as a supplicant, and an access point is called as an authenticator in IEEE 802.1x literature. In the IEEE 802.1x, authentication is performed using EAP (Extensible Authentication Protocol), and the most widely used authentication protocol is EAP-TLS (EAP-Transport Layer Security).[5,6] According to the result of authentication, a port allocated to a supplicant in the authenticator is either closed or open. With EAP-TLS, an authentication server and a supplicant authenticate each other and also they share a secret which is called PMK (Pairwise Master Key). The secret is later transferred from the authentication server to the authenticator via secure channel. Shared secret to establish the secure channel between the authentication server and the authenticator can be setup manually or automatically. After the authenticator obtains the secret resulted from EAP-TLS, it performs 4-way handshake protocol of IEEE 802.11i with a supplicant to make a session key called PTK (Pairwise Transient Key).

Currently, IEEE 802.11i defines a pre-authentication, which performs authentication procedure in advance with neighbor access points that the station associated is likely to roam to via Distribution System (DS). Thus, when the station roams to one of the access points pre-authenticated, they execute the key confirmation 4-way handshake. To increase the hit ratio, logging database system must be used. However, the pre-authentication requires additional overhead cost for IEEE 802.1x authentication with RADIUS server, and also, there are some problems for proper handling of pre-authenticated ports. The additional overhead cost is sometimes useless if the station does not roam to the APs that are pre-authenticated.

When handover occurs, New Access Point can detect the handover from re-association request message that contains the Old Access Point's BSSID. IEEE 802.11f is currently working for development of IAPP using the re-association request. The purpose of the work is to define a framework to exchange information between access points, where the information would be useful for QoS and for security. Especially, they define the Layer2 Update Frame so that any layer 2 devices, e.g., bridges, switches and other APs, can update their forwarding tables with the correct port to reach the new location of the station.

They provide only the vehicle to convey the information, but they do not define what the information should be. The container of the information is called as context block in IEEE 802.11f of which definition is responsible for the context block users.

Recently, many proposals on fast authenticated handover have been appeared. Mishra, et al. proposed a proactive key distribution scheme to support fast and secure roaming, where they raised a question on the perfect forward secrecy.[13] Perfect forward secrecy guarantees that compromise of one access point would not compromise past or future key material. However, their scheme involves RADIUS server interaction besides the standard flow of messages. Also, private information called MK must be installed and shared between RADIUS server and each station. Similarly, Harkins proposed a fast re-authentication method, where New Access Point obtains a PMK from RADIUS server also.[14] Moskowitz defines a blob that includes PMK related information and he uses it to transfer PMK to neighbor access points and a station.[15] It also requires RADIUS server intervention to allocate a PMK per access point.

III. Fast Authentication and Key Exchange during Handover

When a supplicant that is authenticated at an Old Access Point moved to a New Access Point, it must do whole authentication and key exchange procedures again. If a proof for the authentication at the Old Access Point is securely sent to the New Access Point, the supplicant does not need to do the repeated authentication. Also, if a PMK (Primary Master Key) of IEEE 802.11i in the Old Access Point is sent to the new Access Point in a

secure fashion, the supplicant and the New Access Point can establish a secure channel without the help of RADIUS server. In this section, we propose a faster authentication and key exchange scheme using the Context Block in the MOVE-response packet among IEEE 802.11f IAPP messages.

The Context Block of IEEE 802.11f is a series of information elements and we define the Context Block for the protocol as figure 1. Assume that a supplicant that is authenticated at an Old Access Point moved to a New Access Point. Using the Context Block, we define the fast re-authentication and key-exchange procedure as following:

(1) New Access Point recognizes the handover from the reassociate request message and finds BSSID (Basic Service Set IDentifier). RADIUS server lets the New Access Point know the IP address of the BSSID, and the New Access Point communicates with the Old Access Point using the IP address.
(2) New Access Point sends a MOVE-notify IAPP packet to Old Access Point. The MOVE-notify packet contains MAC address of the supplicant and the NULL Context Block.
(3) Old Access Point checks if the supplicant with the MAC address is registered in it. If it is true, Old Access Point sends a MOVE-response packet including the following context block to New Access Point. After sending the MOVE-response packet, Old Access Point deletes PMK from its table. Note that according to IEEE 802.11f, the MOVE-response packet is protected with ESP (IP Encapsulating Security Payload) during the transmission. Thus, an attacker cannot neither modify the context block nor find the PMK.
(4) New Access Point checks if the Context Block indicates the supplicant asking re-association is authenticated. If it is true, New Access Point obtains PMK and performs the 4-way handshake procedure of IEEE 802.11i for generation of pairwise key. By doing this, New Access Point can find out whether the station is authenticated user or not before completing the 4-way handshake. This early authentication capability of stations prevents DOS attack against access points. The feature is useful where rogue stations appear frequently. If both the New Access Point and the supplicant have the same PMK, the 4-way handshake will be completed without error. As the result of the handshake, they share PTK, which is different from the PTK of Old Access Point.
(5) After completing the handshake, New Access Point and the supplicant execute group key distribution protocol using the pairwise key in step 2.

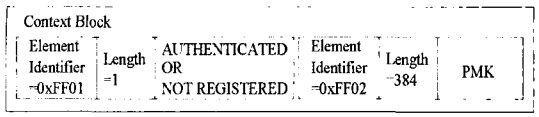

Figure 1 Context Block for Authenticated Handover

The handover that adopted our scheme has several advantages over the usual handover scheme. The former is much faster than the latter, because it alleviates an execution of authentication and key exchange protocol between a supplicant and a RADIUS server. EAP-TLS as the authentication and key exchange protocol is widely used, and the amount of computation and traffic required is quite large compared with the amount of time required for seamless handover. Our scheme can substitute for the pre-authentication of IEEE 802.11i for the devices not supporting the pre-authentication. Also, whenever the pre-authentication is not used because the station roams to another access point, our scheme can substitute for the failed pre-authentication to enhance performance. Because the Context Block is included in a MOVE-response packet and the packet is always sent to New Access Point in the IEEE 802.11f context, no protocol overhead is added to implement the scheme.

Ⅳ. 4-way Handshake with Perfect Forward Secrecy

The proposed scheme in the previous section has a drawback that Old Access Point has access capability to the traffic between the station and New Access Point because it knows the PMK if it did not delete the PMK in its table. Also, if the PMK of Old Access Point is compromised, the traffic between New Access Point and station is also revealed, because they share the PMK. For the environment where the problem is critical or where the perfect forward secrecy is required, we propose

a modified version of 4-way handshake protocol of IEEE 802.11i.

In our proposal, to generate a PTK, the elliptic curve version of the authenticated Diffie-Hellman key exchange protocol is integrated into the 4-way handshake. The reason that we choose the elliptic curve cryptosystem is that the size of Nonce is only 256 bit-long. Currently, only the public-key cryptosystem that can be implemented in 256-bit key space is the elliptic curve cryptosystem. Also, the Diffie-Hellman key exchange consumes only 3.12ms for 163 bit GF(p) elliptic curve cryptography on 450-MHz Pentium-III.[17] Because the Diffie-Hellman key exchange is vulnerable to the man-in-the-middle attack, the public values exchanged between a station and New Access Point must be authenticated in any way. PMK is used for the protection of the first message of the 4-way handshake from active attackers. That is, an MIC using PMK is calculated over the first EAPOL-Key message to guarantee integrity of the first message. MICs over the other three messages are computed using PTK as before, but the PTK is independent of PMK and is computed from the Diffie-Hellman key exchange. Every access point and station share an elliptic curve and a generating point G when they are initially configured. To exchange the key, ANonce is computed by xG where x is randomly selected and kept secret. Similarly, SNonce is computed from secretly selected y. By adopting this authenticated key exchange, we do not need anticipate the man-in-the-middle attack without PKI(Public Key Infrastructure). The modified 4-way handshake is as following:

(1) Authenticator → Supplicant: EAPOL-Key(ANonce = xG, MIC_{PMK})
(2) Supplicant → Authenticator: EAPOL-Key(SNonce = yG, MIC_{PTK})
(3) Authenticator → Supplicant: EAPOL-Key(ANonce, MIC_{PTK})
(4) Supplicant → Authenticator: EAPOL-Key(MIC_{PTK}), where PTK = PRF-X(xyG, "Pairwise key expansion", Min(AA, SA) || Max(AA, SA) || Min(ANonce, SNonce) || Max(ANonce, SNonce))

After the 4-way handshake is successfully completed, a group key distribution protocol using the PTK is executed. The modified 4-way handshake can be implemented on the existing hardware and software architecture only by changing the method of computing PTK.

Early execution of this 4-way handshake is possible in a similar way of the pre-authentication via DS. By doing early handshake, additional overhead in runtime is eliminated. Our scheme is also applicable to other pro-active key distribution protocols in order to support perfect forward secrecy.

V. Utilization of Proactive Caching

To enhance the performance of handover, proactive caching scheme is suggested by.[13] In the proactive caching scheme, authentication and key related information is transferred to neighboring access points while a station associates to an access point. When the station roams to one of the access points that caches previously, they can start immediately 4-way handshake without IEEE 802.1x authentication. However, their approach involves authentication server and accounting server for the caching. Also, it requires pre-distribution of secret key between authentication server and a station to provide perfect forward secrecy. The enforcement of sharing secret key is inconvenient feature because a station must always keep carrying the secret and because authentication server compromise reveals users secret.

If we use the proactive caching strategy, the transfer time of Context Block during re-association is saved. Using the Cache-notify/Cache-response packet, the Context Block containing the authentication proof and the PMK can be delivered to neighboring access points while the station is associated to an access point. If the station roams to the access point that has cached the Context Block, they can immediately start the 4-way handshake. The Context Block is defined as figure 1 to give neighboring access points the proof of authentication and the PMK.

VI. Performance Enhancement

Performance enhancement obtained from the scheme is due to the elimination of EAP-TLS during handover. If our scheme is not used when the pre-authentication is

missed or when the pre-authentication is not implemented, the station must perform re-authentication procedure, and consequently, data transfer will halt during the IEEE 802.11 authentication and association, the IEEE 802.1x authentication, and IEEE 802.1x key management. The adaptation of our scheme eliminates one full EAP-TLS authentication and key exchange or key agreement procedure. A full TLS handshake requires a number of time consuming operations such as certificate validation, certificate revocation list validation, signature generation, public key encryption and decryption, hash operation and ASN.1 decoding for parsing of X.509. Besides that, EAP-TLS involves communication of RADIUS server and EAP packet processing. Thus, the elimination of one EAP-TLS during handover makes it possible to authenticate and exchange keys without halting data transfer during handover. Because the Context Block is included in a MOVE-response packet and the packet is always sent to New Access Point in the IEEE 802.11f context, no protocol overhead is added to implement the scheme. Note that IEEE 802.11f is necessary for a Distribution System of IEEE 802.11 to be supported and for the restriction that a station has a single association at a given time.

The modified version of 4-way handshake increases the amount of computation required for ECDH, but the added computation is small enough (only 3.12ms for 163 bit GF(p) elliptic curve cryptography on 450-MHz Pentium-III) not to affect overall latency of handover. Also, early-4-way handshake may be used to remove the overhead during handover.

To evaluate our authenticated handover scheme, a possible maximum velocity is computed. We compare the result with the pre-authentication. Figures and expressions of calculating maximum velocity are excerpted from.[16] Refer to[16] for more detail.

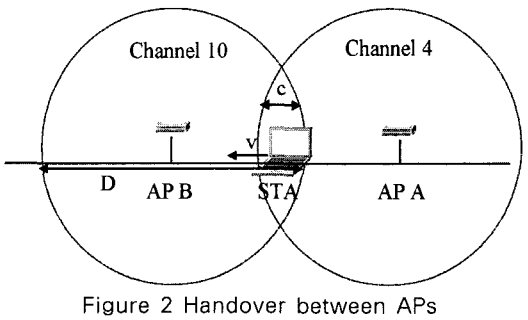

Figure 2 Handover between APs

- Maximum velocity (Pre-authenticated: no PMK cached on New Access Point)
  - $v = c/\ \Delta T_{PA}$
  - $\Delta T_{PA} = \Delta T_{SCAN} + \Delta T_{802.1X} + \Delta T_{4way} + \Delta T_{REASSOC}$
  - Example: c = 2 ft; ΔT = 250 ms (fast resume), V=8 ft/sec (5.5 MPH, pedestrian)
  - If STA can learn of alternative APs via other mechanisms (e.g. advertisement over IP), then c~D.
- Maximum velocity (Pre-authenticated: PMK cached on New Access Point)
  - $v = c/\ \Delta T_{PA}$
  - $\Delta T_{PA} = \Delta T_{SCAN} + \Delta T_{4way} + \Delta T_{REASSOC}$
  - Example: c = 2 ft; ΔT = 100 ms, V=20 ft/sec (13.6 MPH)
- Maximum velocity (Our scheme with ECDH overhead)
  - $v = c/\ \Delta T_{OURS}$
  - $\Delta T_{OURS} = \Delta T_{SCAN} + \Delta T_{4way} + \Delta T_{REASSOC} + \Delta T_{ECDH}$
  - Example: c = 2 ft; ΔT = 103.12 ms, V=19.4 ft/sec (13.2 MPH)

At the sacrifice of only small amount of overhead, our scheme provides perfect forward secrecy without intervention of RADIUS server. Compared with the pre-authentication, our scheme always shows good performance. The pre-authentication cannot always guarantee hit of PMK caching. If the perfect forward secrecy is not required, our scheme always shows the equivalent maximum velocity as the velocity the pre-authentication shows when the cache hits.

Ⅶ. Conclusion and Further Study

We propose a method to use the Context Block of IEEE 802.11f for authenticated handover for seamless services. The method is applicable to devices not supporting the pre-authentication of IEEE 802.11i, and also it can be used for the case that the pre-authentication is failed. Also, we solve the open problem of perfect forward secrecy in pre-authentication of IEEE 802.11 handover by integrating ECDH into the 4-way handshake. With the scheme, a station can handover in a pre-authenticated manner without anticipating information leakage.

We did not mention changes of accounting mechanism

in this paper, but it must be considered because the accounting client in access points changes whenever handover occurs. The new accounting client must let RADIUS server know the change, and some proper action must be taken for the correct accounting.

Acknowledgement

이 논문은 2003학년도 인하대학교의 지원에 의하여 연구되었음.(INHA-30354).

References

[1] Draft Amemdment to STANDART FOR Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control(MAC) and physical layer(PHY) specifications: Specification for Enhanced Security, IEEE Std 802.11i/D5.0, August 2003.

[2] Standards for Local and Metropolitan Area Networks: Standard for Port based Network Access Control, P802.1X/D11, March 27, 2001.

[3] Draft IEEE Standard for Local and Metropolitan Area Networks - Port Based Network Access Control - Amendment 1: Technical and Editorial Corrections, IEEE Draft P802.1aa/D5, February 27, 2003.

[4] Draft Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation, IEEE P802.11F/D5, January, 2003.

[5] RFC 2284, PPP Extensible Authentication Protocol (EAP). L. Blunk, J. Vollbrecht. March 1998.

[6] RFC 2716, PPP EAP TLS Authentication Protocol. B. Aboba, D. Simon. October 1999.

[7] RFC 2138, Remote Authentication Dial In User Service (RADIUS). C. Rigney, A. Rubens, W. Simpson, S. Willens. April 1997.

[8] Internet Draft, DIAMETER Base Protocol, Pat R. Calhoun, John Loughney, Eric Guttman, Glen Zorn, Jari Arkko, December 2002.

[9] Internet Draft, EAP Tunneled TLS Authentication Protocol(EAP-TTLS), Paul Funk, Simon Blake-Wilson, November 2002.

[10] Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control(MAC) and physical layer(PHY) specifications, 1997.

[11] Internet Draft, Microsoft's PEAP version 0, Vivek Kamath, October 2002.

[12] RFC 3078, Microsoft Point-to-Point Encryption, G. Pall, G. Zorn, March 2001.

[13] Arunesh Mishra, Minho Shin, William Arbaugh, Proactive Key Distribution to support fast and secure roaming, IEEE 802.11-03/084, Jan., 2003.

[14] Dan Harkins, Fast Re-authentication, IEEE 802.11-03/095

[15] Robert Moskowitz, PMK Plumbing for Fast Roaming via the Neighborhood Graph, IEEE 802.11-03/411, May, 2003.

[16] Bernard Aboba, Fast Handoff Issues, IEEE 802.11-03/155, March, 2003.

[17] Multiprecision Integer and Rational Arithmetic C/C++ Library, http://indigo.ie/~mscott/#benchmark.

〈著者紹介〉

양 대 헌 (DaeHun Nyang)
1994년 2월 : 한국과학기술원 과학기술대학 전기 및 전자 공학과 졸업
1996년 2월 : 연세대학교 컴퓨터 과학과 석사
2000년 8월 : 연세대학교 컴퓨터 과학과 박사
2000년 9월~2003년 2월 : 한국전자통신연구원 정보보호연구본부 선임연구원
2003년 2월~현재 : 인하대학교 정보통신대학원 전임강사
<관심분야> 암호이론, 암호프로토콜, 인증 프로토콜, 무선 인터넷 보안