WIRELESS COMMUNICATIONS AND MOBILE COMPUTING
Wirel. Commun. Mob. Comput. 2008; **8**:921–925
Published online 17 August 2007 in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/wcm.538

Selecting transition process for WLAN security

Shih-Feng Hsu[1] and Yi-Bing Lin[1,2,*,†]

[1]*Department of Computer Science, National Chiao Tung University, Hsinchu, Taiwan*
[2]*Institute of Information Science, Academia Sinica, Nankang, Taipei, Taiwan*

Summary

In wireless local area network (WLAN), a station (STA) accesses the Internet through an access point (AP). When switching from one AP to another, the STA executes the transition process, which may incur long delay and result in force-termination for real-time applications. The IEEE 802.11r proposes the fast basic service set (BSS) transition to speed up the transition process for a STA moving within the same mobility domain (MD). This scheme requires unique MD assignment so that the STA knows whether it should conduct fast BSS transition process (for intra-MD scenario) or the expensive initial MD association process (for inter-MD scenario). However, how to guarantee unique MD identifier (MDID) assignment is not mentioned in the specification. This paper proposes a mechanism for IEEE 802.11r fast transition without using MDID, and therefore eliminates the cost for MDID management. Copyright © 2007 John Wiley & Sons, Ltd.

KEY WORDS: authentication; authorization and accounting (AAA); fast basic service set (BSS) transition; pairwise transient key (PTK); security; wireless LAN

1. Introduction

Wireless local area network (WLAN) was originally designed for cable replacement. In recent year, WLAN functionality has been extended for users with mobility and has even been integrated with cellular system to serve as an access technology to the cellular system, and therefore scales up the coverage of mobile services. To offer commercial mobile operations with WLAN, several mobile telecommunications network issues, e.g., mobility management [1–3], voice quality [4], and power saving [5], must be addressed in the WLAN environment. Among them, security is probably one of the most important and essential issue that must be carefully addressed. This paper will focus on transition process for WLAN security.

In IEEE 802.11 WLAN, a station (STA; Figure 1 (1)) accesses the Internet through an access point (AP; Figure 1 (2)) over the air [6,7]. Because WLAN is much easier to be intercepted than a wired network, it is important to exercise authentication and encryption between the STA and the AP with a security key. If the STA and the AP are not assigned the same security key through an offline process, the key must be generated in the transition process. When an STA connects to an AP for the first time or switches from one AP to another, the transition process consisting of the following four procedures is exercised.

- *IEEE 802.11 open system authentication* is performed between the STA and the AP. The AP will grant any authentication request from the STA

*Correspondence to: Yi-Bing Lin, Department of Computer Science, National Chiao Tung University, Hsinchu, Taiwan.
†E-mail: liny@csie.nctu.edu.tw

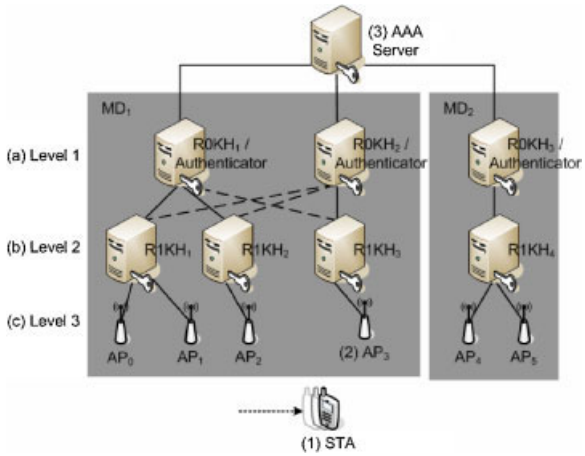

Fig. 1. IEEE 802.11r security hierarchy.

unless the open system authentication is disabled in the AP.

- *Association* enables the STA and the AP to negotiate the security policy and the encryption algorithm.
- *IEEE 802.1X authentication* is executed between the STA and an authentication, authorization, and accounting server (AAA server; Figure 1 (3)) [8]. A master session key (MSK; or AAA-Key) is generated independently in both the STA and the AAA server.
- *IEEE 802.11i 4-way handshake* generates the pairwise transient key (PTK) from the MSK. This PTK provides data integrity and confidentiality by encrypting data transmitted between the STA and the AP.

This transition process may incur long delay and result in force-termination for real-time applications such as voice over IP. To reduce the latency for security key generation in the transition process, IEEE 802.11r proposed fast basic service set (BSS) transition implemented in a three-level key hierarchy [6]. In this hierarchy, the first-level key is Pairwise Master Key first level (PMK-R0) derived from the MSK and is shared between the STA and the PMK-R0 Key Holder (R0KH; Figure 1 (a)). The R0KH is the authenticator that maintains the MSK received from the AAA server. The second-level key is PMK second level (PMK-R1) shared between the STA and the PMK-R1 Key Holder (R1KH; Figure 1 (b)). PMK-R1 is derived from PMK-R0 and is used to derive PTK at the third-level (i.e., the AP; Figure 1 (c)).

Mobility domain (MD) is defined in this three-level key hierarchy. An MD consists of several R0KHs. Figure 1 illustrates two mobility domains MD_1 and MD_2. MD_1 consists of two R0KHs (i.e., $R0KH_1$ and $R0KH_2$) and MD_2 consists of one R0KH (i.e., $R0KH_3$). Each R0KH directly associates with several nearby R1KHs that can acquire PMK-R1 from this R0KH. In Figure 1, $R0KH_1$ directly associates with two R1KHs (i.e., $R1KH_1$ and $R1KH_2$; the connectivity is represented by solid links) and $R0KH_2$ directly associates with one R1KH (i.e., $R1KH_3$). An R1KH can obtain PMK-R1 from an R0KH which does not directly associate with this R1KH, if both key holders are in the same MD. In Figure 1, $R1KH_1$ and $R1KH_2$ can acquire PMK-R1 from $R0KH_2$, and this indirect association is represented through the dashed links. Based on the MD structure, there are three STA transition scenarios: intra-R1KH transition (e.g., from AP_0 to AP_1 in Figure 1), inter-R1KH transition in an MD (e.g., from AP_1 to AP_2 or AP_3), and initial MD association (or inter-MD transition; e.g., from AP_3 to AP_4) scenarios. In this paper, the third scenario is described in Section 2. The first two scenarios are intra-MD scenarios described in Section 3. Section 4 proposes a selection mechanism that automatically selects the appropriate transition process for intra- and inter-MD scenarios.

2. Initial MD Association Process (Inter-MD Scenario)

When an STA first associates to the WLAN or moves from one MD to another (inter-MD transition), PMK-R0 and PMK-R1 for this STA are generated and stored in the R0KH and the R1KH, respectively [6]. Assume that an STA first connects to AP_1 in Figure 1. The steps in Figure 2 are executed as follows.

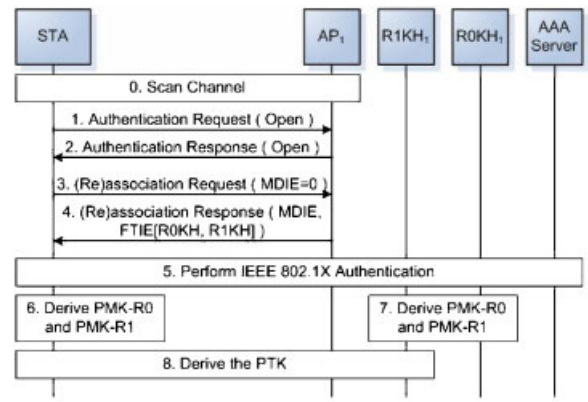

Fig. 2. IEEE 802.11r initial MD association process.

DOI: 10.1002/wcm

Step 0. The STA scans multiple channels for an AP with good signal, and checks the information elements (IEs) advertised in the signal (i.e., Beacon and Probe Response frames). If the mobility domain IE (MDIE) is included in the frames, it means that the AP supports the IEEE 802.11r fast BSS transition. The MDIE contains the mobility domain identifier (MDID) of MD_1 and the transition policy.

Steps 1 and 2. Suppose that AP_1 is selected. The STA sends an authentication request message to AP_1 and performs the open system authentication.

Steps 3 and 4. The STA sends an association request message to AP_1. In this message, the MDIE field is set to 0 to indicate that the initial MD association process is exercised. AP_1 replies an association response message to indicate the MDID of MD_1, and fast BSS transition IE (FTIE) which includes the identifiers of $R0KH_1$ and $R1KH_1$.

Step 5. The IEEE 802.1X authentication is executed between the STA and the AAA server. A new MSK is independently generated in the STA and the AAA server. This key is also passed from the AAA server to $R0KH_1$.

Steps 6 and 7. The STA and $R0KH_1$ independently generate the PMK-R0 key by executing the key derivation function (KDF; Figure 3 (1)) with the $R0KH_1$ identifier, the MSK (generated at Step 5), the MD_1 identifier, and the supplicant address (SPA; the STA's Medium Access Control (MAC) address). Then PMK-R1 is derived from PMK-R0, SPA, and the $R1KH_1$ identifier (Figure 3 (2)).

Step 8. The STA and AP_1 perform the IEEE 802.11i 4-way handshake procedure by exchanging two random numbers (i.e., ANonce generated by AP_1 and SNonce generated by the STA). To derive PTK, AP_1 sends the related parameters to $R1KH_1$, including the $R0KH_1$ identifier, SNonce, ANonce, and SPA. Then the STA and $R1KH_1$ independently derive the PTK key from inputs including the PMK-R1 generated at Steps 6 and 7 (Figure 3 (3)). After PTK is generated, $R1KH_1$ passes it to AP_1 for encrypting and decrypting data transmitted between the STA and AP_1.

After this initial MD association process, PMK-R0 and PMK-R1 are kept in $R0KH_1$ and $R1KH_1$, respectively. When the STA moves to another AP in MD_1, these two keys are reused to generate new PTK without executing the IEEE 802.1X authentication.

3. Fast BSS Transition (Intra-MD Scenarios)

The IEEE 802.11r fast BSS transition is exercised in intra-MD transition scenarios. When the STA performs inter-R1KH transition from AP_1 to AP_3 in MD_1, the following steps are executed (see Figure 4).

Step 1. Since AP_1 and AP_3 are in the same MD, the STA sends an authentication request message with fast BSS transition (FT) authentication to AP_3. This message contains the MDID of MD_1 and FTIE (containing the $R0KH_1$ identifier and a random number SNonce for PTK derivation).

Step 2. From the MDIE and the FTIE provided by the STA, AP_3 knows that the inter-R1KH transition occurs. AP_3 sends an authentication response message to the STA. This response message contains the identifiers of $R0KH_2$, $R1KH_3$, MD_1, and a random number ANonce for deriving PTK.

Step 3. Upon receipt of ANonce and the identifiers from AP_3, the STA generates a new PMK-R1 key from the $R1KH_3$ identifier, SPA, and PMK-R0 (Figure 3 (2)). This PMK-R1 key is shared between the STA and $R1KH_3$, and is used together with SPA, ANonce, and SNonce to derive the PTK key (Figure 3 (3)). If the STA moves from AP_1 to AP_0 connecting to the

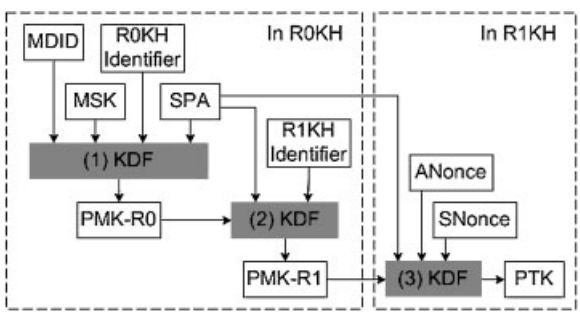

Fig. 3. Derivation of PMK-R0, PMK-R1, and PTK.

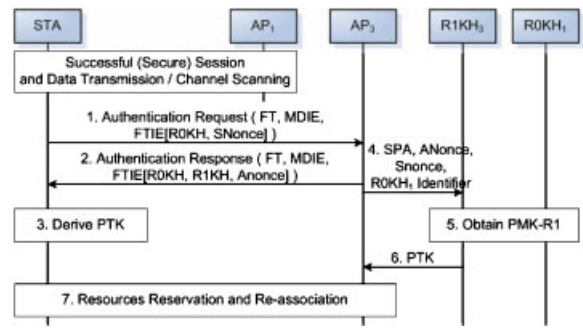

Fig. 4. IEEE 802.11r fast BSS transition process.

DOI: 10.1002/wcm

same R1KH in Figure 1, the old PMK-R1 is reused to generate the new PTK key.

Step 4. AP_3 sends SPA, ANonce, SNonce, and the $R0KH_1$ identifier to $R1KH_3$ for deriving new PTK.

Step 5. According to the $R0KH_1$ identifier, $R1KH_3$ acquires the new PMK-R1 from $R0KH_1$. If the STA moves from AP_1 to AP_0 in Figure 1, this step is omitted.

Step 6. $R1KH_3$ derives PTK by executing KDF (Figure 3 (3)) and sends the generated PTK to AP_3. After this step, PTK is kept in both the STA and AP_3.

Step 7. The STA switches from AP_1 to AP_3 after resource reservation and re-association between the STA and AP_3.

In the fast BSS transition, the IEEE 802.1X authentication procedure is omitted. Instead, PMK-R0 is reused to derive the new PTK key to speed up the transition process.

4. Transition Process Selection Mechanism

Since every AP advertises the MDID in the Beacon and Probe Response frames, the STA can select the appropriate transition process for intra-MD or inter-MD scenarios. Specifically, the MAC addresses are used as the identifiers for R0KH and R1KH to ensure global uniqueness. The MDID is assumed to be managed by vendors [6]. However, it is not clear how to guarantee unique MDID among vendors. If ambiguity of MDID does occur, this error will be detected at Step 5 in Figure 4 because the new PMK-R1 can not be acquired. Therefore the STA is forced to stop the fast BSS transition process and is switched to perform the IEEE 802.11r initial MD association process.

To resolve the ambiguous MDID issue, we propose a new method that does not require the MDID for transition. In our approach, every AP maintains an R0KH table recording all R0KHs that can be accessed by the AP. In Figure 1, the identifiers of $R0KH_1$ and $R0KH_2$ are recorded in AP_0, AP_1, AP_2, and AP_3, and the $R0KH_3$ identifier is recorded in AP_4 and AP_5. Upon receipt of the authentication request message (i.e., Step 1 in Figure 4), an AP queries its R0KH table to determine whether the STA comes from another MD, and selects the appropriate transition process for execution. Suppose that the STA moves form AP_{Old} to AP_{New}. The following steps are executed (see Figure 5).

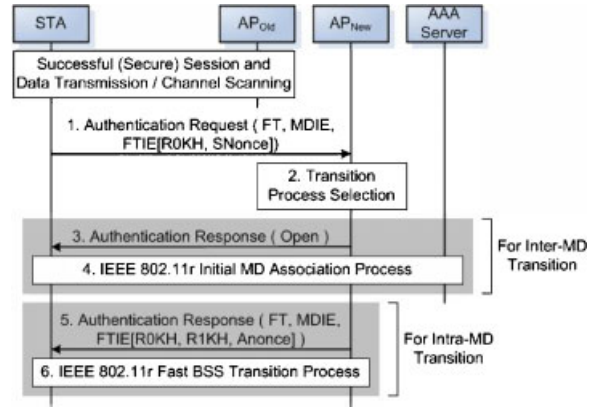

Fig. 5. The proposed selection mechanism for transition process.

Step 1. The STA sends an authentication request message with FT authentication algorithm to AP_{New}. This message is similar to that in Step 1 of Figure 4, but does not include the MDID in MDIE.

Step 2. Upon receipt of the authentication request, AP_{New} checks the R0KH identifier in FTIE. There are two possibilities. If the R0KH identifier is not found in the R0KH table of AP_{New}, Steps 3 and 4 are executed (for inter-MD scenario). Otherwise, Steps 5 and 6 are executed (for intra-MD scenarios).

Steps 3 and 4. AP_{New} exercises open system authentication and replies the authentication response message with parameter 'open system authentication.' Then the STA proceeds to execute the IEEE 802.11r initial MD association process (Steps 2–8 in Figure 2).

Steps 5 and 6. AP_{New} exercises FT authentication and replies the IEEE 802.11 authentication response message with parameter 'FT authentication.' The IEEE 802.11r fast BSS transition process is executed (Steps 2–7 in Figure 4).

Through the R0KH table in an AP, the above mechanism correctly distinguishes the inter-MD scenario from the intra-MD scenarios without using the MDID.

A few other studies have been reported in the literature which have also carried out research similar to that reported in this paper [9–11].

5. Conclusion

This paper describes the IEEE 802.11r transition process for WLAN, where a three-level key hierarchy was proposed to speed up the transition process with-

DOI: 10.1002/wcm

out executing the expensive IEEE 802.1X authentication for some scenarios. This hierarchy requires assignment of unique MDIDs world wide. However, how to guarantee the uniqueness of MDID is not clear. This paper proposed a mechanism that does not need MDID, and therefore MDID management is eliminated. This mechanism also saves four message exchanges incurred in the original fast BSS transition when MDID ambiguity occurs. Detailed performance evaluation of the selection mechanism for transition process will be our future work.

Acknowledgement

This work was sponsored in part by NSC Excellence project NSC 95-2752-E-009-005-PAE, NSC 95-2218-E-009-201-MY3, NSC 95-2221-E-009-024, NSC 95-2219-E-009-010, NSC 95-2219-E-009-019, Intel, Chung Hwa Telecom, IIS/Academia Sinica, ITRI/NCTU Joint Research Center and MoE ATU.

References

1. Ma W, Fang Y, Lin P. Mobility management strategy based on user mobility patterns in wireless networks. *IEEE Transactions on Vehicular Technology* 2007; **56**(1): 322–330.
2. Lin Y-B, Chlamtac I. *Wireless and Mobile Network Architecture*. John Wiley & Sons, Inc., 2001.
3. Lin Y-B. Performance modeling for mobile telephone networks. *IEEE Network* 1997; **11**(6): 63–68.
4. Qian Y, Hu RQ, Chen H-H. A call admission control framework for voice over WLANs. *IEEE Wireless Communications* 2006; **13**(1): 44–50.
5. Yang S-R. Dynamic power saving mechanism for 3G UMTS system. *ACM/Springer Mobile Networks and Applications (MONET)*, November 2006 (online version).
6. IEEE. Draft Amendment to STANDARD for Information Technology—Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Network—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 2: Fast BSS transition. IEEE Std. 802.11r/D4.0, November 2006.
7. Chen J-H, Pang A-C, Sheu S-T, Tseng H-W. High performance wireless switch protocol for IEEE 802.11 wireless networks. *ACM Mobile Networking and Applications* 2005; **10**(5): 741–751.
8. Lin Y-B, Pang A-C. *Wireless and Mobile All-IP Networks*. John Wiley & Sons, Inc., 2005.
9. Pang A-C, Chen Y-K. A study on availability of mobility databases. *International Conference on Information Networking (ICOIN)*, 2004.
10. Kassab M, Belghith A, Bonnin J-M, Sassi S. Fast pre-authentication based on proactive key distribution for 802.11 infrastructure networks. *ACM Wireless Multimedia Networking and Performance Modeling*, October 2005.
11. Bargh MS, Hulsebosch RJ, Eertink EH, Prasad A, Wang H, Schoo P. Fast authentication methods for handovers between IEEE 802.11 wireless LANs. *ACM WMASH 2004*, October 2004.

Authors' Biographies

Shih-Feng Hsu received his B.S.C.S. degree from National Tsing Hua University, Taiwan, R.O.C. in 2001. He is currently a Ph.D. candidate of the Department of Computer Science and Information Engineering, National Chiao Tung University, Taiwan, R.O.C. His current research interests include persional communications services, mobile computing, IMS, and WiMAX.

Yi-Bing Lin is Chair Professor and Dean of College of Computer Science, National Chiao Tung University. His current research interests include mobile computing and cellular telecommunications services. Dr Lin has published over 200 journal articles and more than 200 conference papers. He is the co-author of the books *Wireless and Mobile Network Architecture* (with Imrich Chlamtac; published by Wiley, 2001) and *Wireless and Mobile All-IP Networks* (with Ai-Chun Pang; published by Wiley, 2005). Dr Lin is an IEEE Fellow, ACM Fellow, AAAS Fellow, and IEE Fellow.

DOI: 10.1002/wcm