

國立交通大學  
資訊科學與工程研究所  
碩士論文

支援 IEEE 802.11s 無線區域網狀網路整合式  
安全網域之機制

A Mechanism for Supporting Integrated Security Domain  
for IEEE 802.11s WLAN Mesh Networking

研究生：劉合翰  
指導教授：曾建超 教授

中華民國九十六年七月

支援 IEEE 802.11s 無線區域網狀網路整合式安全網域之機制  
A Mechanism for Supporting Integrated Security Domain for IEEE  
802.11s WLAN Mesh Networking

研究生：劉合翰  
指導教授：曾建超

Student：Ho-Han Liu  
Advisor：Chien-Chao Tseng

國立交通大學  
資訊科學與工程研究所  
碩士論文



A Thesis  
Submitted to Institute of Computer Science and Engineering  
College of Computer Science  
National Chiao Tung University  
in partial Fulfillment of the Requirements  
for the Degree of  
Master  
in  
Computer Science

July 2007

Hsinchu, Taiwan, Republic of China

中華民國九十六年七月

# 支援 IEEE 802.11s 無線區域網狀網路整合式安全網域之機制

學生：劉合翰

指導教授：曾建超 博士

國立交通大學資訊科學與工程研究所碩士班

## 摘 要

本論文針對無線區域網狀網路 (WLAN Mesh)，提出一套機制將 IEEE 802.11i 標準之認證機制及金鑰管理與 WLAN Mesh 環境加以整合。WLAN Mesh 具備不需佈線以及功能強大的繞徑機制，可提供快速與低成本的骨幹網路佈建。然而現有 WLAN Mesh 的安全機制自外於 802.11i，因此換手處理與訊框繞送之效能不佳，足以影響即時性服務之品質。

本論文之機制以不影響 802.11i 之安全性為前提，將 MAP (mesh access point) 的認證者 (authenticator) 功能改設置於 MPP (mesh portal)，降低行動端於換手時執行 IEEE 802.11i 認證之需求。因此，換手延遲與訊息流量將可有效降低，同時加密訊框之繞送效能也獲得改善。此外，本機制可相容於 IEEE 802.11i 標準，不需更動行動端即可達成上述之改良。對於 WLAN Mesh 而言，本機制可與 IEEE 802.11s 標準同時運作，不影響原有之安全機制與繞送機制。

另一方面，本論文提出一分析模型用以計算行動端漫遊於 WLAN Mesh 時，安全程序所衍生之換手延遲與流量。根據計算結果顯示，本機制可降低換手延遲達 245%，並提供等同於 802.11i preauthentication 機制運作於 80%-90% 成功率之效能。此模型亦可運用於分析集中式 WLAN 架構下，認證者與存取點 (access point) 位於不同網路實體時，單一認證者管理存取點數量之最佳值。

**關鍵詞：**整合式安全網域、快速認證、集中式無線區域網路架構、無線區域網狀網路、隨機行走模型


# A Mechanism for Supporting Integrated Security Domain for IEEE 802.11s WLAN Mesh Networking

Student : Ho-Han Liu

Advisor : Dr. Chien-Chao Tseng

Institute of Computer Science and Engineering  
National Chiao Tung University

## ABSTRACT



This thesis proposes a mechanism to integrate the authentication and key management scheme of the IEEE 802.11i standard with the WLAN Mesh environment. WLAN Mesh eliminates the need for cabling and provides a powerful routing mechanism, so that deployments of the backbone network will be faster and less expensive than the wired counterpart. However, the security mechanism of the WLAN Mesh is isolated from 802.11i. This isolation of security mechanism introduces extra overhead in handoff handling and routing, and thus degrades the quality of real-time services.

In order to improve the handoff performance while fulfilling the security requirement of 802.11i, the proposed mechanism makes the mesh portal (MPP), instead of the mesh access point (MAP), the IEEE 802.1X authenticator so that it can reduce the demand for performing the IEEE 802.1X authentication in handoffs. As a consequence, it not only reduces the handoff latency and message traffic but also improves the routing performance of the encrypted frame. Meanwhile, the mechanism is compatible with IEEE 802.11i and can be used by a station without any modification. Furthermore, the mechanism can also operate with IEEE 802.11s, affecting neither the original routing mechanism nor the security mechanism of IEEE 802.11s.

We also propose an analytical model to evaluate the handoff latency and message traffic caused by the security procedures while a station roaming within a WLAN Mesh network. The results show that the proposed mechanism can reduce the handoff latency up to 245% and achieve the same performance as the one accomplished by the 802.11i preauthentication with a successful probability of 80%-90%. Moreover, this model can be further applied in analyzing the optimum number of APs managed by one authenticator in a centralized WLAN architec-

ture, where authenticators and APs are implemented in distinct network entities.

**Keywords:** integrated security domain, fast authentication, centralized WLAN architecture, WLAN Mesh networking, random walk model



## 誌 謝

首先要感謝我的指導教授—曾建超老師這一年半來的悉心指導。老師給予我的研究相當大的激勵，使我深刻體認孜孜矻矻的求學態度乃是一切的根基。我與老師結緣於三年前，當時因緣際會而錯失良機。如今有幸拜入老師的門下，一切要感謝主的安排。

同時要感謝曹孝櫟教授提供精闢的見解與建議，使論文的完整性得以提升。文中 AP deployment 與 MP topology 觀念之釐清、average hop count 影響之分析與 handoff traffic 等內容皆得自於曹老師的啟發。

感謝紀光輝教授與蘇坤良教授於百忙中撥冗審閱，提供寶貴且極具建設性的意見，使本論文臻至完善。雖僅有數面之緣，但我相當感激兩位老師對我的鼓勵與指導。

本篇論文的原始構想，源自於王瑞堂學長（相信大家都稱呼他為 RT）。RT 的熱情、靈活的思緒與豐富的創造力令我十分稱羨，而他更是我的良師益友，與他討論的過程中每每激盪出新的火花。在此祝福他順利取得博士學位。

我要特別感謝張乃心同學。若缺少了她的幫助，資質驚頓的我恐怕無法在短時間內完成分析模型。此外，文中 Figure 2-18、Figure 3-8、Figure 3-9 與 Figure 5-5 亦是出自她的手筆。乃心是我所認識的人之中，插圖畫得最好的一位，第一次聽她報告時，投影片中的插圖與動畫就讓我驚豔不已。乃心與我一起經歷了工研院的專利審查、Mobile Computing 2007 的論文發表與無數次的討論，她一直是我最好的伙伴。

最後，僅以此論文獻給我的父母、外公與外婆，他們是我一切的原點。

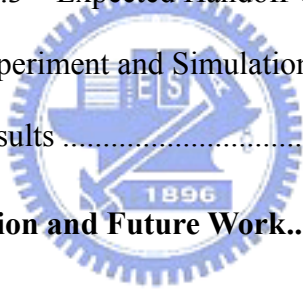
# Contents

<b>Abstract in Chinese</b> .....	<b>i</b>
<b>Abstract in English</b> .....	<b>ii</b>
<b>Acknowledgements</b> .....	<b>iv</b>
<b>Table of Contents</b> .....	<b>v</b>
<b>List of Figures</b> .....	<b>viii</b>
<b>List of Tables</b> .....	<b>xi</b>
<b>Chapter 1 Introduction</b> .....	<b>1</b>
1.1 Motivation .....	1
1.2 Objective.....	2
1.3 Synopsis.....	4
<b>Chapter 2 Background and Related Work</b> .....	<b>5</b>
2.1 WLAN Mesh Networking .....	5
2.2 AP Security Domain .....	6
2.2.1 Architecture .....	6
2.2.2 Authentication .....	8
2.2.3 Key Hierarchy.....	9
2.2.4 RSNA Establishment .....	10
2.3 Mesh Security Domain .....	12
2.3.1 Architecture .....	12
2.3.2 Key Hierarchy.....	13
2.3.3 Initial EMSA Authentication .....	14

2.3.4	Subsequent EMSA Authentication .....	15
2.3.5	Mesh Key Holder Security Association.....	16
2.3.6	EMSA Establishment.....	17
2.4	IEEE 802.11 Handoff .....	19
2.4.1	Handoff Latency .....	20
2.5	Fast Authentication Methods .....	21
2.5.1	Preauthentication .....	21
2.5.2	PMK Sharing .....	23
2.5.2.1	Needham-Schroeder Protocol.....	24
2.5.2.2	Frequent Handoff Region Selection Algorithm....	25
2.5.3	PMK Predistribution.....	27
2.5.3.1	Neighbor Graph Algorithm.....	27
2.5.3.2	Fast BSS Transition .....	30
2.5.4	Summary.....	33
<b>Chapter 3</b>	<b>Integrated Security Domain.....</b>	<b>34</b>
3.1	Architecture .....	34
3.2	RSNA Establishment .....	35
3.3	Handoff Procedures .....	36
3.3.1	Intra-MPP Handoff .....	37
3.3.2	Inter-MPP Handoff .....	38
3.4	Encapsulation.....	39
3.5	Fragmentation Issue.....	44
<b>Chapter 4</b>	<b>Security Considerations.....</b>	<b>46</b>
4.1	Trust Relationship.....	46
4.2	Threat Model .....	49



4.3	Advantages .....	50
<b>Chapter 5</b>	<b>Handoff Overhead Estimation.....</b>	<b>51</b>
5.1	Handoff Model.....	51
5.2	Estimation Equations .....	57
5.2.1	Handoff Latency .....	57
5.2.1.1	Intra-MPP Handoff Latency .....	57
5.2.1.2	Inter-MPP Handoff Latency .....	60
5.2.2	Handoff Traffic .....	63
5.2.2.1	Intra-MPP Handoff Traffic .....	63
5.2.2.2	Inter-MPP Handoff Traffic .....	65
5.2.3	Expected Handoff Overhead.....	66
5.3	Experiment and Simulation .....	67
5.4	Results .....	68
<b>Chapter 6</b>	<b>Conclusion and Future Work.....</b>	<b>74</b>
	<b>Bibliography .....</b>	<b>76</b>



# List of Figures

Figure 1-1	WLAN Mesh security architecture.....	3
Figure 1-2	Scope of PTK .....	3
Figure 2-1	Non-mesh WLAN infrastructure.....	5
Figure 2-2	WLAN Mesh infrastructure.....	6
Figure 2-3	802.1X architecture and protocol stack of ASD.....	7
Figure 2-4	802.1X authentication .....	8
Figure 2-5	Key hierarchy and derivations of 802.11i .....	9
Figure 2-6	PTK structure of TKIP and CCMP .....	10
Figure 2-7	802.11i RSNA establishment.....	11
Figure 2-8	802.1X architecture of the MSD .....	13
Figure 2-9	Key hierarchy and derivations of 802.11s.....	14
Figure 2-10	Initial EMSA authentication.....	15
Figure 2-11	Subsequent EMSA authentication.....	16
Figure 2-12	Mesh key holder security handshake.....	17
Figure 2-13	Overall EMSA establishment .....	18
Figure 2-14	BSS transition.....	19
Figure 2-15	802.11 handoff procedures .....	20
Figure 2-16	802.11i preauthentication .....	22
Figure 2-17	PMK sharing with the Needham-Schroeder protocol .....	24
Figure 2-18	AP placement and FHR.....	25
Figure 2-19	FHR scheme .....	26
Figure 2-20	AP placement and the corresponding neighbor graph.....	28
Figure 2-21	PMK derivations of the neighbor graph algorithm .....	28

Figure 2-22	Neighbor graph algorithm .....	29
Figure 2-23	Key hierarchy and derivations of 802.11r .....	30
Figure 2-24	802.11r initial FT association and PMK-R1 predistribution .....	31
Figure 2-25	Over-the-Air FT authentication .....	32
Figure 2-26	Over-the-DS FT authentication .....	32
Figure 3-1	WLAN Mesh security architecture with ISD .....	34
Figure 3-2	PTK distribution .....	35
Figure 3-3	RSNA establishment with ISD .....	36
Figure 3-4	Intra-MPP handoff .....	37
Figure 3-5	Intra-MPP handoff with ISD .....	37
Figure 3-6	Inter-MPP handoff .....	38
Figure 3-7	Inter-MPP handoff with ISD .....	39
Figure 3-8	TKIP frame encryption processing .....	40
Figure 3-9	CCMP frame encryption processing .....	40
Figure 3-10	Encapsulation processing (external destination) .....	41
Figure 3-11	Encapsulation processing (external source) .....	42
Figure 3-12	Encapsulation processing (internal) .....	43
Figure 3-13	MTU value and fragmentation issue .....	45
Figure 4-1	Trust Relationships in the ASD .....	47
Figure 4-2	Trust Relationships in the MSD .....	47
Figure 4-3	Trust Relationships in the ISD .....	48
Figure 5-1	AP deployment based on the cell structure .....	51
Figure 5-2	Topology of MP services .....	52
Figure 5-3	MAP deployment and cell classification .....	53
Figure 5-4	MP topology of the 3-subarea cluster .....	54
Figure 5-5	State diagram for a 6-subarea cluster .....	55

Figure 5-6	Handoff pattern for ISD and 802.11i.....	56
Figure 5-7	Intra-MPP handoff latency with ISD.....	58
Figure 5-8	Intra-MPP handoff latency with 802.11i.....	59
Figure 5-9	Inter-MPP handoff latency with ISD.....	61
Figure 5-10	Inter-MPP handoff latency with 802.11i.....	62
Figure 5-11	Intra-MPP handoff traffic with ISD.....	63
Figure 5-12	Intra-MPP handoff traffic with 802.11i.....	64
Figure 5-13	Inter-MPP handoff traffic with ISD.....	65
Figure 5-14	Inter-MPP handoff traffic with 802.11i.....	66
Figure 5-15	Experimental environment.....	67
Figure 5-16	Handoff latency with different $P_{PF}$ .....	69
Figure 5-17	Handoff latency with different $n$ .....	69
Figure 5-18	Handoff latency of ISD with different $n$ and $P_{PF}$ .....	70
Figure 5-19	Improvement of ISD with different $n$ and $L_{IX}$ .....	70
Figure 5-20	Relationship between ISD and 802.11i in the equal $L_S$ .....	71
Figure 5-21	Handoff latency with different $H$ .....	71
Figure 5-22	Handoff traffic with different $P_{PF}$ .....	72
Figure 5-23	Handoff traffic with different $n$ .....	72
Figure 5-24	Handoff traffic with different $H$ .....	73

## List of Tables

Table 5-1	Parameters measured in the experimental platform.....	68
Table 5-2	Average $P_{REVISIT}$ calculated in the simulation .....	68



# Chapter 1

## Introduction

### 1.1 Motivation

The growth of the IEEE 802.11-based device creates a tremendous business opportunity and huge requirements for the WLAN infrastructure. A WLAN consist of access points (APs) which communicate with stations (STAs) via radio links, but are wired to switches. WLAN Mesh eliminates the need for cabling so that deployments are faster and less expensive. WLAN Mesh supports automatic topology learning and dynamic path selection, and the network can organize by itself. Some wireless ISPs have adopted the WLAN Mesh infrastructure to provide widely Internet access. An example deployed by Q-ware Systems Inc. in Taipei City is WIFLY, which consists of 4000 APs and is the broadest coverage of wireless broadband Internet in the world.

To secure the WLAN communication, wired equivalent privacy (WEP) is proposed by the IEEE 802.11 working group to provide authentication, integrity, and encryption. However, cryptographers have identified many flaws in WEP, such as manual key management, keystream reusing and CRC-32 message authentication. Many Wi-Fi hotspots may apply the HTTPS authentication to control the network access. Nevertheless, the absence of per-packet authenticity makes the network vulnerable to the MAC address spoofing. Therefore, deploying IEEE 802.1X and IEEE 802.11i standards [10], [12] are necessary for the WLAN environment.

The handoff latency is critical to WLAN because real-time services are sensitive to delay and jitter. The inter-AP handoff takes a few hundred milliseconds and damages the quality of real-time communication. Unfortunately, the problem is further aggra-

vated in the robust security network (RSN). It costs 750-1200 milliseconds [3] for an STA to execute full 802.1X authentication in the inter-AP handoff.

Mechanisms [6], [13], [15]-[19] have been proposed to remove the 802.1X authentication latency and reduce the handoff overhead. These mechanisms either require sharing the pairwise master key (PMK) among APs, which will result in serious security flaws, or need precisely target AP prediction to help STAs preauthenticate with the correct AP, or introduce new key hierarchies which are not compatible with the conventional devices. In this research, a security mechanism is proposed to integrate the security domains of WLAN Mesh and remove the overhead caused by link layer security protocols.

## 1.2 Objective

A security domain means a set of network entities on which a single security policy is employed by a single administrative authority [20]. As shown in Figure 1-1, a WLAN Mesh is composed of two security domains: mesh security domain (MSD) and AP security domain (ASD). A mesh portal (MPP) and mesh points (MPs) connecting to this MPP define an MSD; a pair of mesh access point (MAP) and STA defines an ASD. The security mechanism is different in the MSD and the ASD. Mesh links among MPs is protected by the 802.11s standard [14], but the connection between an STA and an MAP is protected by the 802.11i standard.

After an STA switched its serving MAP, the trustworthiness of the new MAP has to be ascertained by the STA, and vice versa. This is carried out by the reauthentication service. What is important at this stage is to determine the trustworthiness and establish a security association between each other.

Since EAP methods, e.g. PEAP and EAP-TTLS, are not optimized for reauthentication, the overhead of 802.1X authentication certainly contributes to the handoff la-

tency. Previous researches for this issue only focus on the ASD. They neither integrate with the WLAN Mesh infrastructure nor deal with the routing overhead caused by security mechanisms in the multi-hop network.

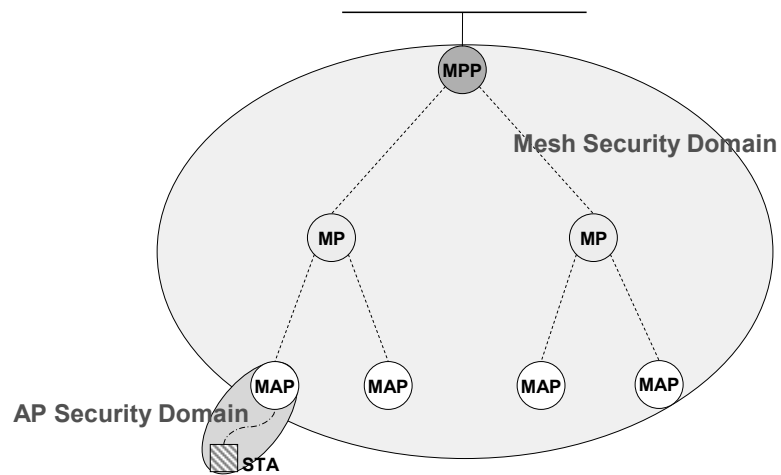


Figure 1-1 WLAN Mesh security architecture

The routing performance in the multi-hop network suffers from the separated security architecture. As shown in Figure 1-2, due to the scope of pairwise transient key (PTK) is limited in a single hop, MPs on the routing path have to decrypt frames first and re-encrypt them with the next-hop PTK before forwarding. Such “hop-by-hop” processes not only incur overhead to MPs but also degrade the quality of real-time services seriously.

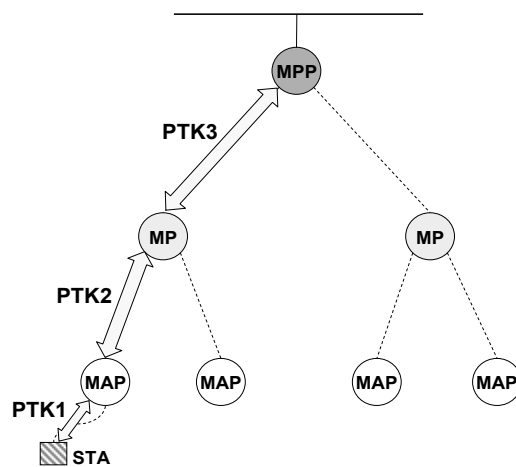


Figure 1-2 Scope of PTK



The objective of this research is to enhance the security mechanism of WLAN Mesh to improve the QoS for real-time services. It is achieved by reducing the handoff latency and eliminating the routing overhead caused by encryption processing. The proposed security mechanism should fulfill the following requirements:

1. Assure the security of 802.11i RSN.
2. Remove 802.1X authentication from handoff procedures.
3. Establish an end-to-end security channel between an STA and an MPP.
4. Avoid modifying STAs, including software and hardware.
5. Cooperate with the 802.11s standard.

### **1.3 Synopsis**

The remainder of this thesis is organized as follows. Chapter 2 introduces background technologies and related works. Chapter 3 presents the proposed mechanism, including system architecture and message flows. The security analysis and the estimated handoff latency are presented in chapter 4 and chapter 5. At last, we conclude this research and introduce our future works in chapter 6.

## Chapter 2

### Background and Related Work

We begin this chapter by describing the system architecture and the security mechanism of WLAN Mesh, following by analyzing handoff procedures and latency. Finally, related works are discussed.

#### 2.1 WLAN Mesh Networking

The WLAN infrastructure usually consists of APs connecting to a wired network providing wireless connectivity for STAs. The non-mesh WLAN deployment model is illustrated in Figure 2-1.

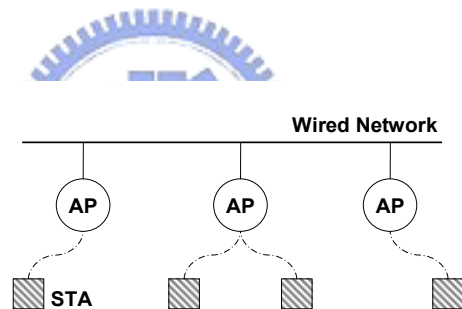


Figure 2-1 Non-mesh WLAN infrastructure

An example of the WLAN Mesh infrastructure is shown in Figure 2-2. A WLAN Mesh is an 802.11-based wireless distribution system (WDS) consisting of a set of MPs interconnected via wireless links. An MP may be collocated with an AP to provide both mesh services and AP services in a single device referred to as MAP. STAs have to associate with an MAP to access the WLAN Mesh.

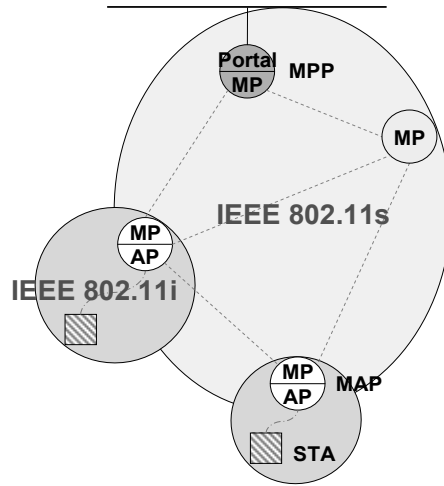


Figure 2-2 WLAN Mesh infrastructure

MPs and MAPs participate in operations of the mesh networking, but STAs do not. Two security mechanisms operate independently in the MSD and the ASD; hence the security architecture of WLAN Mesh is divided into two domains.

## 2.2 AP Security Domain

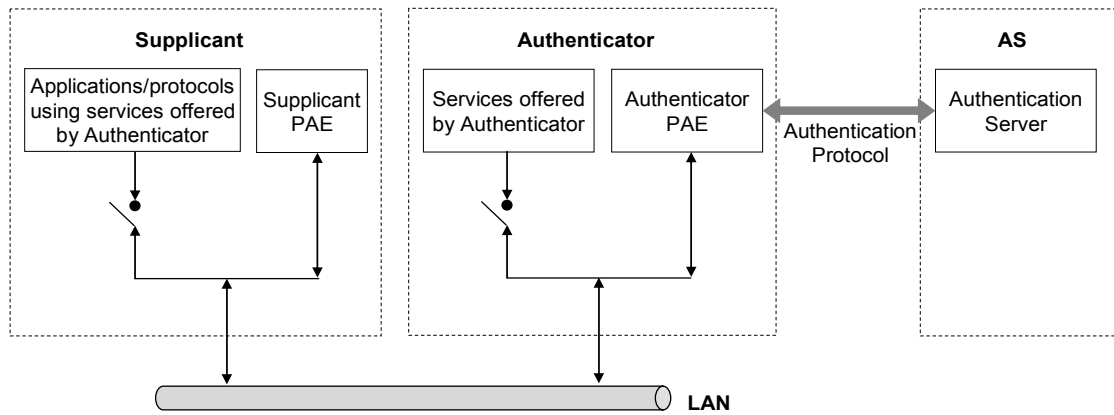
The security mechanism of ASD consists of 802.1X authentication, 4-way handshake and encryption protocols, i.e. TKIP and CCMP. The security mechanism is designed to establish a robust security network association (RSNA) between an STA and an MAP for securing the wireless connection.

Due to the delay of the ratification to 802.11i, Wi-Fi protected access (WPA), a subset of the 802.11i standard, is adopted by the Wi-Fi Alliance as a transitional solution to WEP insecurities. WPA2 is the full implementation of the 802.11i standard and provides a robust security protocol for WLAN.

### 2.2.1 Architecture

There are three components defined by 802.1X. As shown in Figure 2-3, the supplicant is an STA which requests to access WLAN Mesh. The authenticator is the serving MAP which controls the access to the network and blocks unauthorized traffics. The authen-

tication server (AS), e.g. a RADIUS server, provides authentication services for checking the credentials of the supplicant on behalf of the authenticator.



EAP			
EAPOL		EAPOL	RADIUS
802.11		802.11	802.3
			UDP/IP
			RADIUS
			802.3
			UDP/IP

Figure 2-3 802.1X architecture and protocol stack of ASD

802.1X provides the port-based network access control for authenticating devices attached to a LAN port. Ports on an 802.1X-capable device are switched between authorized state and unauthorized state. A port is enabled while in the authorized state, or disable, while in the unauthorized state. The 802.1X specification permits initialization traffics, such as DHCP messages, to pass the port in the unauthorized state.

The protocol stack of 802.1X is illustrated in Figure 2-3. On the top is the EAP layer which includes the EAP protocol and EAP methods. The EAP protocol is a framework allows EAP methods to perform authentication transactions between the supplicant and the AS. EAP messages are carried by EAPOL frames transmitted between the supplicant and the authenticator. All EAP messages are encapsulated into RADIUS packets and forwarded to the AS for further processing.

## 2.2.2 Authentication

The message flows of 802.1X authentication are shown as Figure 2-4. Detail procedures are as follows:

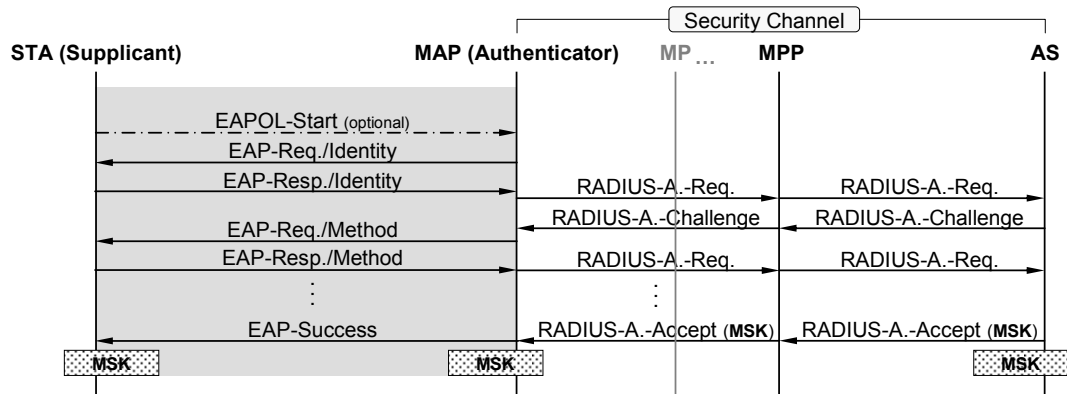


Figure 2-4 802.1X authentication

1. An 802.1X authentication may be initialized by an EAPOL-Start message sent by the STA or an EAP-Request/Identity message sent by the MAP.
2. The STA responds the user identifier with an EAP-Response/Identity message, and the identifier is encapsulated into a RADIUS-Access-Request packet and forwarded to the AS.
3. The AS issues an authentication challenge. This challenge is passed to the STA as an EAP-Request/Method message for negotiating the EAP method used later.
4. The STA and the AS exchange the authentication information carried by EAP-Request/Respond messages. This step may be repeated many times depending on the EAP method.
5. After finishing the EAP authentication, both the STA and the AS generate a master session key (MSK). For authorizing the serving MAP, the MSK is distributed from the AS to the MAP via the security channel.
6. In the end, a RADIUS-Access-Accept packet is passed to the STA as an

EAP-Success message for indicating that the 802.1X authentication is complete.

### 2.2.3 Key Hierarchy

After an STA passed the 802.1X authentication, it is authorized to access the network, and the communication between the STA and its serving MAP should to be secured. In order to provide data encryption and integrity for the 802.11 connection, a key hierarchy is adopted by the 802.11i standard to derive a session key. Figure 2-5 illustrates the key hierarchy and derivations.

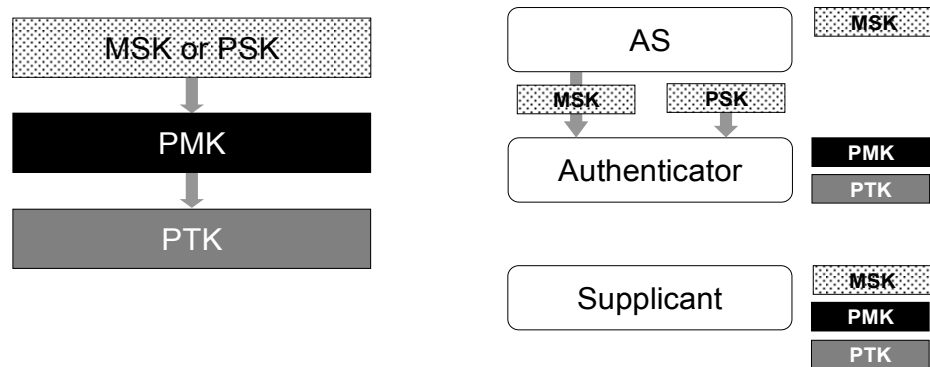


Figure 2-5 Key hierarchy and derivations of 802.11i

An MSK or a PSK is the highest order keys never exposed to any other party except the AS, the authenticator and the supplicant. The MSK is generated by the EAP method and consists of two portions: Enc-RECV-Key and Enc-SEND-Key. The supplicant and the authenticator may either take the Enc-RECV-Key or the PSK as a PMK. The PTK is a session key derived from the PMK, which collaborates with TKIP or CCMP to provide confidentiality, integrity and origin authenticity.

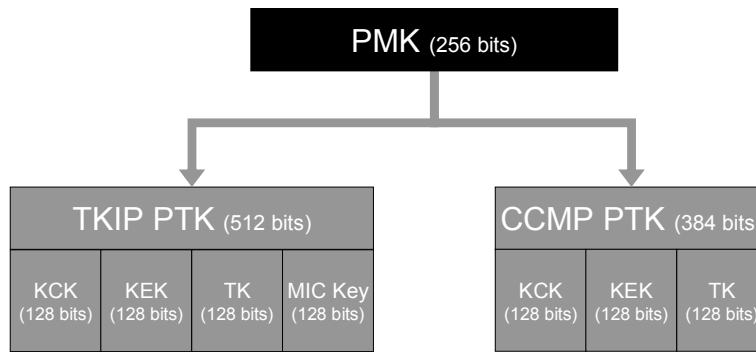


Figure 2-6 PTK structure of TKIP and CCMP

802.11i defines two structures of PTK. As shown in Figure 2-6, both of TKIP and CCMP start with the EAPOL key confirmation key (KCK) used to compute the message integrity check of the EAPOL-Key message. After that is the EAPOL key encryption key (KEK) used to encrypt the EAPOL-Key message. The temporal key (TK), is used for data encryption. Since TKIP is designed to be compatible with the traditional encryption and authentication scheme of WEP, it requires an additional key to perform the Michael integrity check (MIC). For CCMP, the TK is used for both data encryption and integrity check.

#### 2.2.4 RSNA Establishment

An STA has to first establish the RSNA with its serving MAP and is able to access WLAN Mesh. The procedures of RSNA establishment consist of 802.1X authentication and 4-way handshake. Figure 2-7 shows the message flows of RSNA establishment, where the MPP is not involved but forwards the authentication information to the AS.

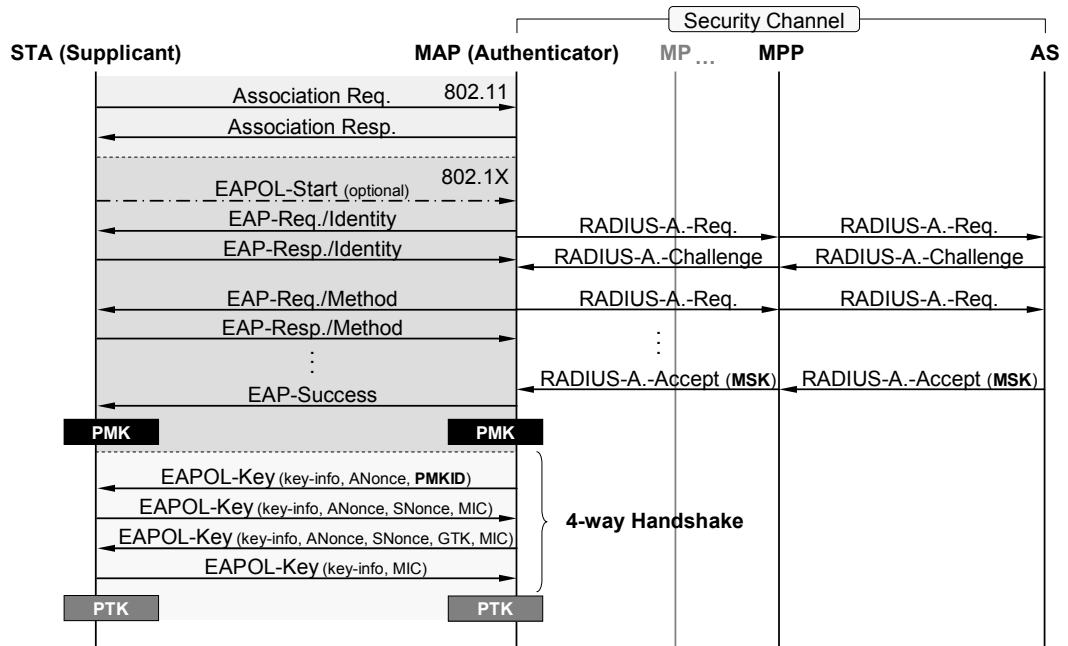


Figure 2-7 802.11i RSNA establishment

1. After associating with the MAP, the STA performs 802.1X authentication.
2. The AS and the STA obtain an MSK from the EAP method. The AS distributes the MSK to the MAP.
3. The STA and the MAP derive a PMK from the MSK. If the PSK is used instead of the PMK, 802.1X authentication will be skipped.
4. The STA and the MAP perform 4-way handshake. To prevent replay attacks the MAP sends ANonce to the supplicant with message #1. The PMKID is also included in this message for synchronizing the PMK used in the handshake. Message #1 is neither encrypted nor authenticated, and thus the response missing or mismatching will fail the handshake.
5. The STA derives a fresh PTK and sends SNonce and robust security network information element (RSNIE) to the MAP with message #2. This message is authenticated with the MIC calculated by the STA with the KCK.
6. The MAP derives the symmetric PTK and checks the integrity of message #2. If the MIC is invalid, the handshake fails, otherwise the MAP acknowledges



the STA that the PTK is successfully derived. In addition, a GTK could be also distributed to the STA with message #3.

7. The STA responds a confirmation to the MAP for informing that the PTK is installed. Message #4 is authenticated with the KCK, too.
8. After establishing the RSNA, the MAP switches the 802.1X port to the authorized state, and thus the network access is allowed.

## 2.3 Mesh Security Domain

The efficient mesh security association (EMSA) proposed by 802.11s secures mesh links between an MP and its peers, which includes EMSA authentication, 4-way handshake, key distribution and encryption protocols.

### 2.3.1 Architecture

The 802.1X architecture of MSD is essentially the same as ASD. However, since an MP is capable of utilizing and providing the distribution service, the roles of supplicant and authenticator are both adopted by the MP.



Figure 2-8 illustrates the 802.1X architecture of MSD. If MP A requires making use of the services provided by MP B, MP A's supplicant PAE has to be authenticated by MP B's authenticator PAE, and vice versa. Therefore, without the EMSA, an MP needs to perform enormous 802.1X authentications to establish the link security with peer MPs. For instance, an MP in the fully connected WLAN Mesh with 5 MPs and 10 mesh links will perform 8 rounds of 802.1X authentication.

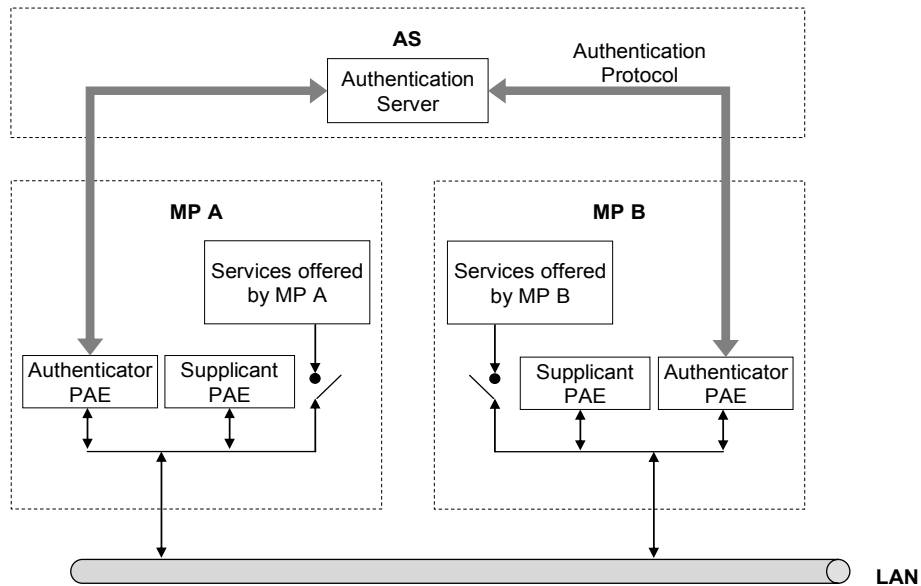


Figure 2-8 802.1X architecture of the MSD

EMSA services permit two MPs efficiently establish the link security without performing 802.1X authentication. There are two types of mesh key holders defined by the EMSA: mesh authenticators (MAs) and mesh key distributors (MKDs). The functions of the 802.1X authenticator are distributed between MKD and MA. An MP may implement one type or both.

### 2.3.2 Key Hierarchy

802.11s also introduces a new key hierarchy. As shown in Figure 2-9, an MSK or a PSK is the highest order key never exposed to any other party except the AS, the MKD and the supplicant MP. Under that the key hierarchy splits into two branches.

The left portion is the link security branch which provides keys for authentication and encryption between a supplicant MP and an MA. The functions of the PMK are divided into PMK-MKD and PMK-MA. The PMK-MKD is a proof that the supplicant has been authenticated. The PMK-MA is used to derive the session key and is generated by the MKD for each MA respectively. Separating the PMK functions is able to simplify following authentications for subsequent mesh link establishments.

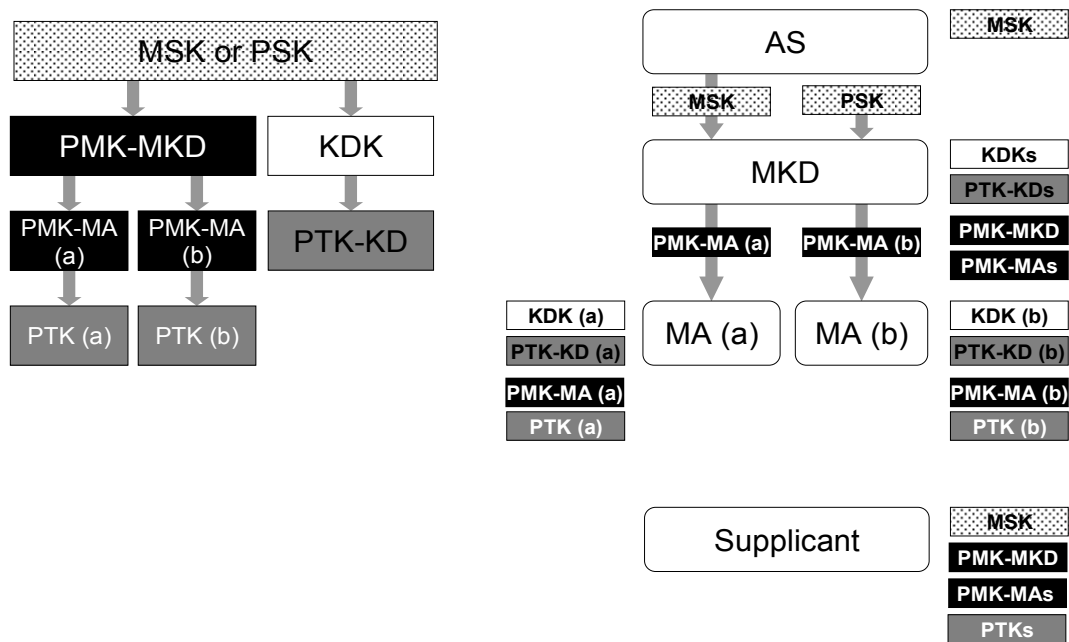


Figure 2-9 Key hierarchy and derivations of 802.11s

The right portion is the key distribution branch which provides keys to secure the distribution of PMK-MAs between an MKD and MAs. The KDK is a proof that the MA and the MKD have established the security association. The PTK-KD is the session key derived from the KDK to secure the PMK-MA distribution.

### 2.3.3 Initial EMSA Authentication

A supplicant MP which has not established any security association needs to perform the initial EMSA authentication to establish the EMSA with the MA. Moreover, a mesh key hierarchy is also constructed in both the supplicant MP and the MA. Figure 2-10 explains the initial EMSA authentication, where the MA (a) is an MKD.

1. The supplicant MP performs full 802.1X authentication with the MA (a). RADIUS messages are forwarded via the MPP.
2. The MSK is distributed from the AS to the MKD.
3. According to the mesh key hierarchy, the MKD and the supplicant MP derive the PMK-MKD and the PMK-MA (a)
4. The supplicant MP and the MA (a) perform 4-way handshake to derive the

PTK (a). Procedures of 4-way handshake are the same as the RSNA establishment described in section 2.2.4.

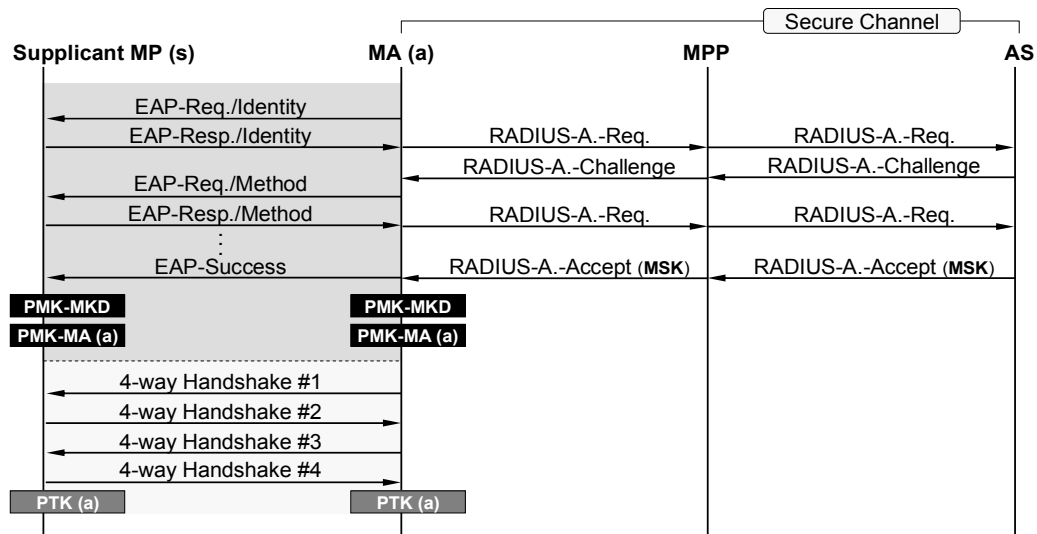


Figure 2-10 Initial EMSA authentication

### 2.3.4 Subsequent EMSA Authentication

Once a mesh key hierarchy is established, an MP performs the subsequent EMSA authentication to establish security associations with peer MPs. The 802.1X authentication is removed, and thus multiple mesh links can be established efficiently. The message flows of the subsequent EMSA authentication are shown as Figure 2-11.

1. The supplicant MP derives the PMK-MA (b) from the PMK-MKD generated in the initial EMSA authentication.
2. The MA (b) requests the PMK-MA (b) from the MKD, i.e. MA (a).
3. The MKD derives the PMK-MA (b) and encrypts it with the PTK-KD (b). After that, the PMK-MA (b) is distributed to the MA (b) with a PMK-MA Delivery Pull Mesh Action frame.
4. Once the supplicant MP and the MA (b) have the PMK-MA (b), they will perform 4-way handshake to derive the PTK (b).

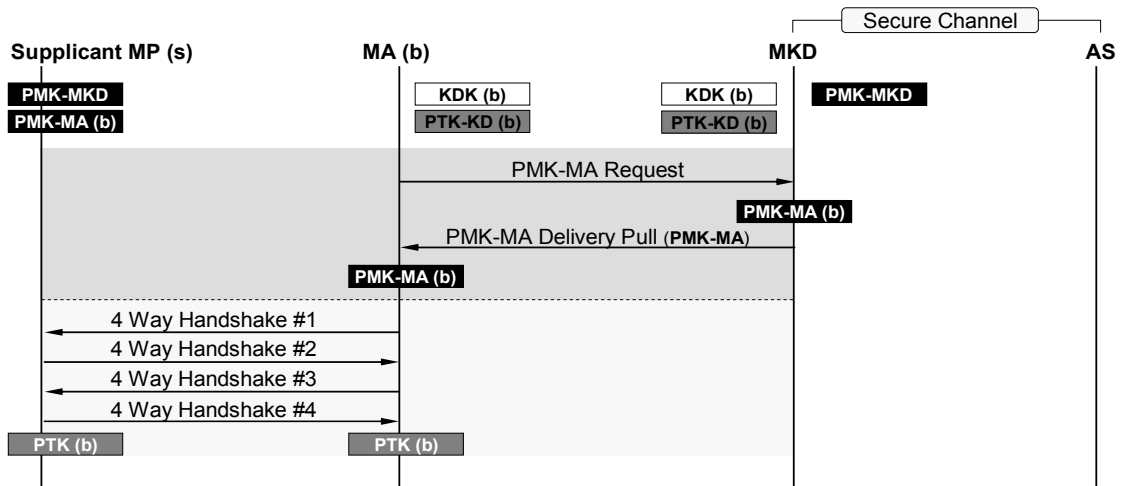


Figure 2-11 Subsequent EMSA authentication

The PTK-KD (b) is derived from the mesh key holder security handshake. Detail procedures of the handshake are described in the next section.

### 2.3.5 Mesh Key Holder Security Association

The mesh key holder security association provides data integrity and origin authenticity for the EAP authentication message transmitted between MA and MKD. Furthermore, it secures the distribution of PMK-MA and facilitates subsequent EMSA authentication.

After the supplicant MP passed the initial EMSA authentication, it can access the mesh network via the MA (a). However, if the supplicant MP further needs to operate as an MA, it has to establish the mesh key holder security association with the MKD. Figure 2-12 illustrates the message flows of the mesh key holder security handshake, where the MKD is the MA (a) mentioned in the previous section.

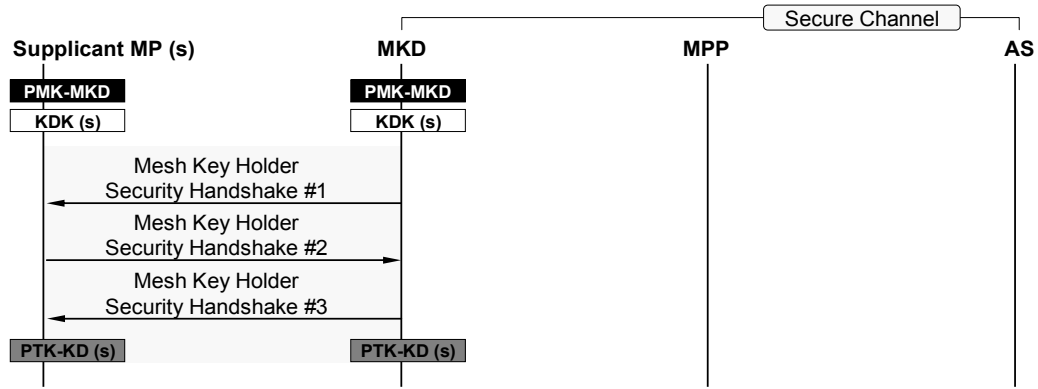


Figure 2-12 Mesh key holder security handshake

The mesh key holder security association start with the discovery of the MKD, followed by the 3-way handshake initiated by the MKD. After the handshake, a PTK-KD is derived from the KDK, and the supplicant MP (s) is able to provide the MA service. Frames transmitted between MA and MKD, such as the PMK-MA distribution, are encrypted by the PTK-KD.

### 2.3.6 EMSA Establishment

The overall message flows of the EMSA establishment and mesh key holder security association are shown in Figure 2-13, where the MKD and MAs are implemented at different MPs.

1. The supplicant MP establishes a mesh link with the MA (a) and performs full EAP authentication.
2. Since the MA (a) is not the MKD, all EAP messages are forwarded to the MKD with the mesh EAP message transport protocol. The MKD encapsulates EAP messages into RADIUS packets and forwards to the AS.
3. After the EAP authentication, the MKD constructs the mesh key hierarchy and distributes the PMK-MA (a) to the MA (a).
4. The MA (a) and the supplicant MP perform 4-way handshake to derive the PTK (a).

5. The supplicant MP continues to establish another mesh link with MP (b). The subsequent EMSA authentication is performed.
6. The supplicant MP establishes the mesh key holder security association with the MKD.
7. After all, two mesh links between are established, and the supplicant MP is ready to provide the MA service.

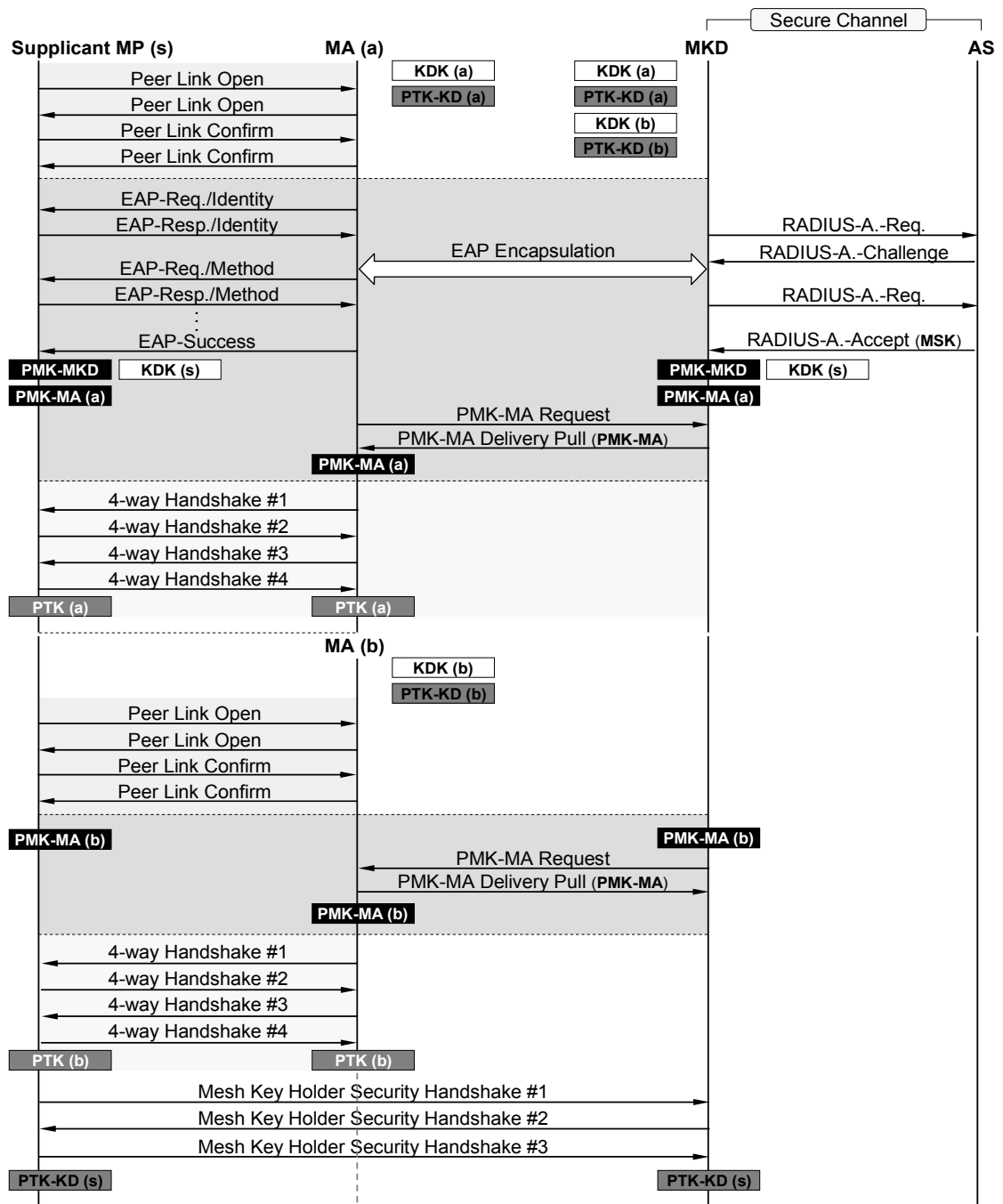


Figure 2-13 Overall EMSA establishment

## 2.4 IEEE 802.11 Handoff

Mobility is an inherent characteristic of the wireless networking. However, all wireless transmissions have a limited geographical range. The transmission range of an 802.11 AP is typically a few hundred feet. Upon moving out of the range of the current associated AP, an STA enters into the range of another AP and performs handoff procedures to regain the connectivity.

Handoff mechanisms are designed to deal with STAs moving between APs, so that the continuous and QoS-guaranteed communication is supported. The 802.11 standard provides the mobility support for STAs traveling between basic service sets (BSSs), but not the extended service set (ESS).

Transitions between APs can be categorized into three types:

1. No transition. STAs move within the signal range of the current AP, no further considerations are needed.
2. BSS transition. STAs drop the connection to the current AP and then reassociate with another AP in the same ESS. To reconnect to the distribution system (DS), STAs need to be authenticated by the new AP. Figure 2-14 gives an example of the BSS transition.

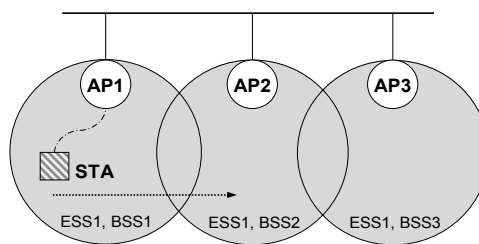


Figure 2-14 BSS transition

3. ESS transition. STAs move from one AP to another AP in a distinct ESS. Higher-layer mobility management protocol, such as Mobile IP, is necessary



to support the seamless handoff. The ESS transition is out of scope of this research.

### 2.4.1 Handoff Latency

Handoff latency is the amount of time that the connectivity between an STA and the DS is lost. 802.11 handoff procedures consist of four portions: discovery phase, commit phase, authentication phase and handshake phase, where authentication phase and handshake phase are only introduced in the network applying 802.1X and 802.11i.

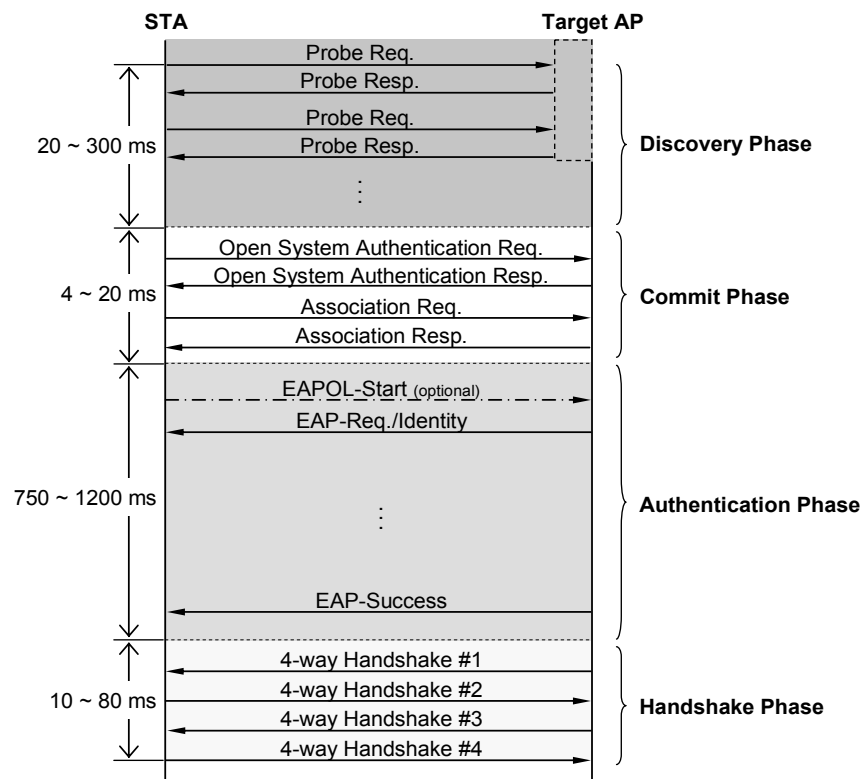


Figure 2-15 802.11 handoff procedures [5]

Because of signal strength decreasing or transmission errors, an STA decides to handoff to the target AP. In the discovery phase, the STA performs the active scan to construct a candidate AP list. The handoff algorithm chooses the “best” AP from the list to be the target AP and controls the STA to associate with it. Following that is the commit phase; the STA authenticates (open system) and associates with the target AP to establish an 802.11 link. Current handoff latency in the non-802.11i environment is too

long to support real-time services<sup>1</sup>; nevertheless, the authentication phase makes it worse. The research [5] indicates that about 75% to 95% of the handoff latency is contributed by the 802.1X authentication.

802.1X authentication is composed of time-consuming mathematical operations. The EAP protocol needs several message round-trips to exchange the authentication information and derive keys. For example, the PEAP/EAP-MSCHAPv2 protocol requires 22 EAPOL messages. Moreover, authentication messages may be transmitted over the Internet while the AS resides in the remote network. Therefore, to support the seamless handoff, the substantial latency incurred by the 802.1X authentication must be eliminated.

## **2.5 Fast Authentication Methods**

The issue of 802.1X authentication has been addressed. Some methods have been proposed to mitigate the overhead of 802.1X authentication and improve the handoff performance. Previous works are discussed in this section.

### **2.5.1 Preauthentication**

With the preauthentication mechanism proposed by 802.11i, an STA is allowed to perform 802.1X authentication with a new AP before associating with it. The preauthentication separates the commit phase from the authentication phase and permits them to be performed independently.

Because an STA can only associate with an AP at a time, preauthentication messages transmitted between the STA and the target AP are forwarded via the current AP. Figure 2-16 shows the procedures of the 802.11i preauthentication.

---

<sup>1</sup> Improvements for reducing the latency of the discovery phase have been proposed.

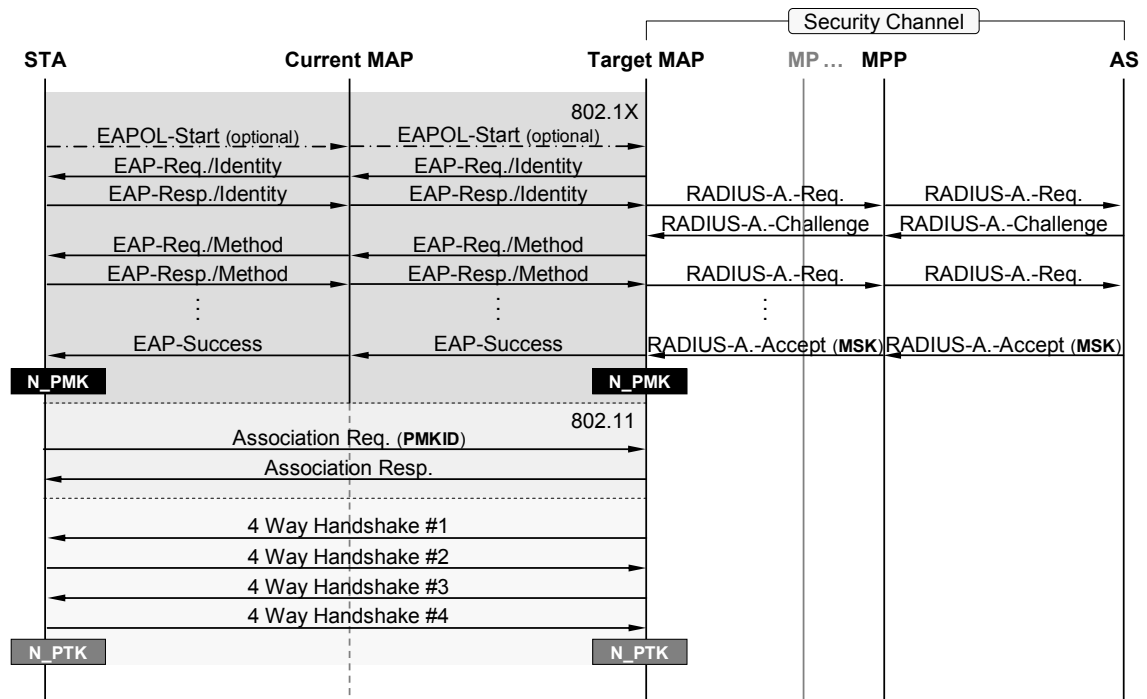


Figure 2-16 802.11i preauthentication

1. 802.11i preauthentication start with an EAPOL-Start message sent from the STA to the target MAP. Except all EAPOL messages are forwarded via the current MAP, the procedures are identical to the 802.1X authentication described in section 2.2.2.
2. After the preauthentication complete, a new PMK (N\_PMK) is derived. The STA and the target MAP cache this N\_PMK for further usage.
3. While associating with the target MAP, the STA inserts the PMKID into the Association Request frame to indicate that the N\_PMK is cached. If the PMKID is valid, the target MAP will skip 802.1X authentication and initialize 4-way handshake directly.

The benefit of preauthentication is that the 802.1X authentication is independent of the handoff procedures. An STA is able to authenticate with multiple candidate APs. However, preauthentication establishes authentication state and key management state on both the STA and candidate APs. To avoid the storage cost and the overhead of pre-

authentication burden AP and AS, STA should only preauthenticate with the AP that it is most likely to handoff to. Therefore, precisely target AP prediction is necessary for STA to perform preauthentication efficiently.

On the negative side, preauthentication is expensive in terms of computational power and latency for STA. The 802.1X authentication latency actually is not reduced by the preauthentication. To guarantee the QoS for real-time applications, an STA needs to perform preauthentication early enough before the current connection is dropped. Thus, well designed and overlapping coverage areas are essential to perform preauthentication successfully. In addition, preauthentication introduces opportunities for DoS attacks. Malicious STAs could burden the AS by preauthenticating with a large number of APs.

## 2.5.2 PMK Sharing

PMK sharing mechanisms intend to reduce the authentication latency by distributing the PMK in use to candidate APs before the handoff. If the PMK is cached by the target AP, 802.1X authentication can be removed. PMK sharing mechanisms reduce not only the handoff latency, but also the overhead of AS and mesh network.

However, with PMK sharing mechanisms, a PMK is possible shared by all APs in the same ESS. Although the PMK mostly is encrypted during the distribution, the key transfer protocol still weakens the security of 802.11i RSN. A compromised PMK may affect all APs in the ESS. Moreover, sharing the PMK means that all APs in the ESS are capable of obtaining the content of the encrypted communication between an STA and its associated AP, which violates the 802.11i trust assumption<sup>2</sup>. On the other hand, modifications are needed for an STA to recalculate the PMKID of the shared PMK at different APs.

---

<sup>2</sup> Only the current associated AP is trusted by the STA, all other non-associated APs are not.

### 2.5.2.1 Needham-Schroeder Protocol

Jan et al. proposed a key distribution mechanism [15] adopting the Needham-Schroeder protocol to distribute a PMK among APs. Each AP and AS have a distinct symmetric key  $K$ , and thus AS can securely distribute the PMK to the AP.

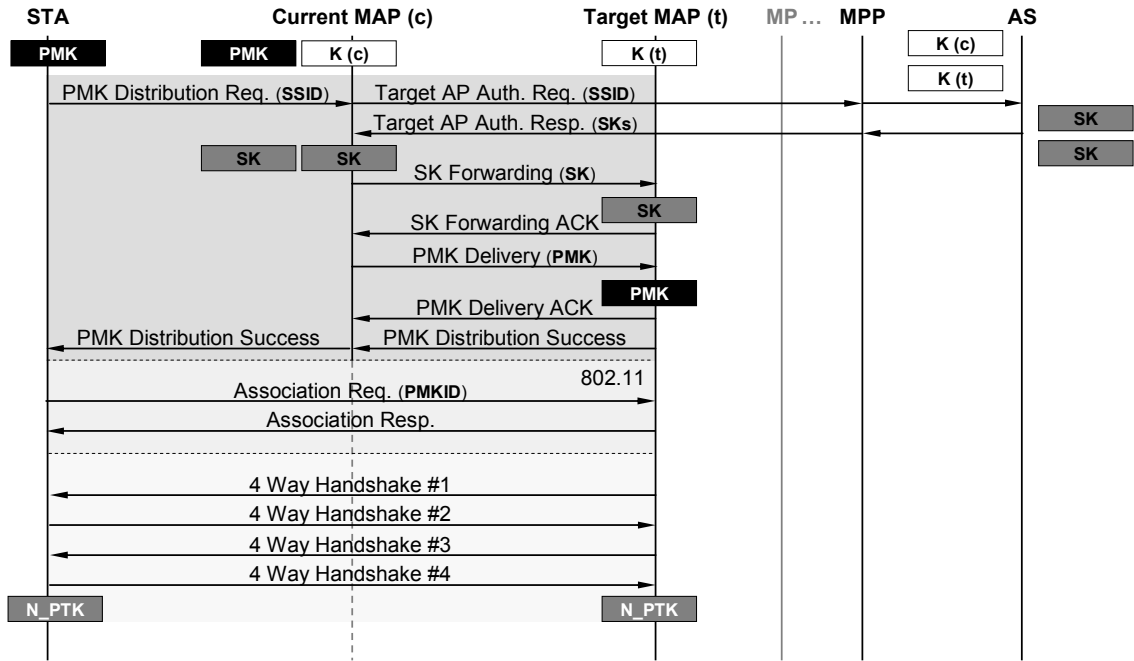


Figure 2-17 PMK sharing with the Needham-Schroeder protocol

Figure 2-17 illustrates the procedures of the PMK distribution. Details are as follows:

1. The STA sends a request message to the current MAP. The SSID of the target MAP is included in this message.
2. The current MAP verifies the identity of the target MAP via the AS. If the target is legit, a session key SK is distributed to two MAPs. A security channel is constructed with the SK.
3. The PMK is transmitted from the current MAP to target MAP via the security channel.
4. A message is sent by the target MAP to inform the STA that the PMK distri-

bution is complete.

5. After the PMK distribution, the target MAP skips 802.1X authentication and performs 4-way handshake with the STA.

### 2.5.2.2 Frequent Handoff Region Selection Algorithm

Pack et al. proposed a predictive handoff scheme referred to as frequent handoff region (FHR) scheme [19]. To reduce the authentication latency, an MSK is proactively distributed to multiple APs depending on the STA's mobility pattern. The FHR selection algorithm is also introduced to determine the subset of adjacent APs perhaps visited by the STA in the near future.

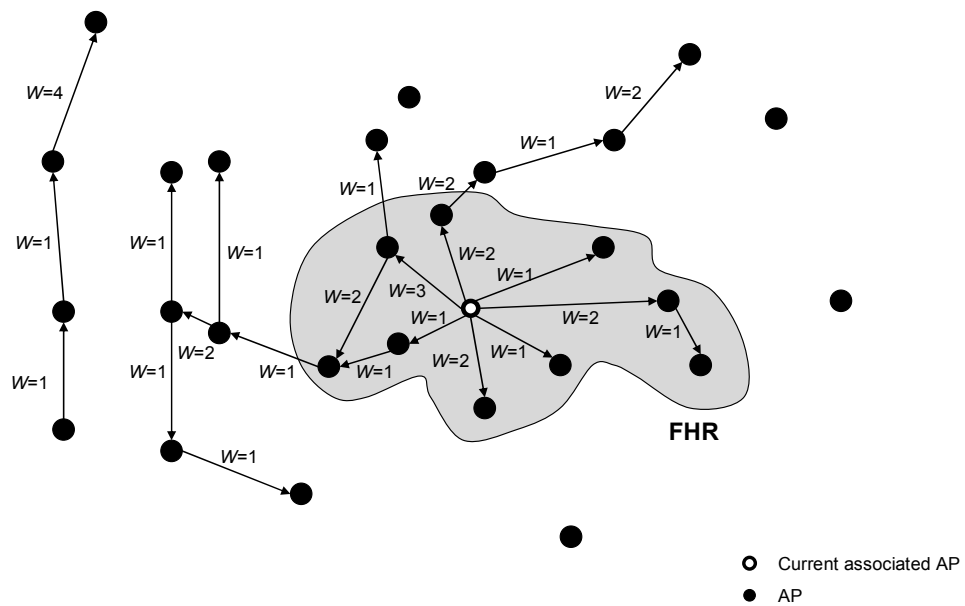


Figure 2-18 AP placement and FHR

Based on the historical handoff behaviors, a weighted directed graph of the AP placement shown in Figure 2-18 is constructed.

The weight value between the  $AP_i$  and the  $AP_j$  is defined as  $W(i, j)$ , where

$$W(i, j) = \begin{cases} 0, & i = j \\ \frac{1}{H(i, j)}, & i \neq j, AP_i \text{ and } AP_j \text{ are adjacent} \\ \infty, & AP_i \text{ and } AP_j \text{ not are adjacent} \end{cases} \quad (1)$$

$$H(i, j) = \frac{N(i, j)}{R(i, j)} \quad (2)$$

$N(i, j)$  denotes the number of handoff events from the  $AP_i$  to the  $AP_j$ .  $R(i, j)$  denotes the residential time in the  $AP_i$  before STAs handoff to the  $AP_j$ .

The number of APs selected into the FHR is limited by the weight value and the maximum hop count. Figure 2-18 gives an example of a FHR selected with the criterion that the weight value upper bound is 3 and the maximum hop count is 2.

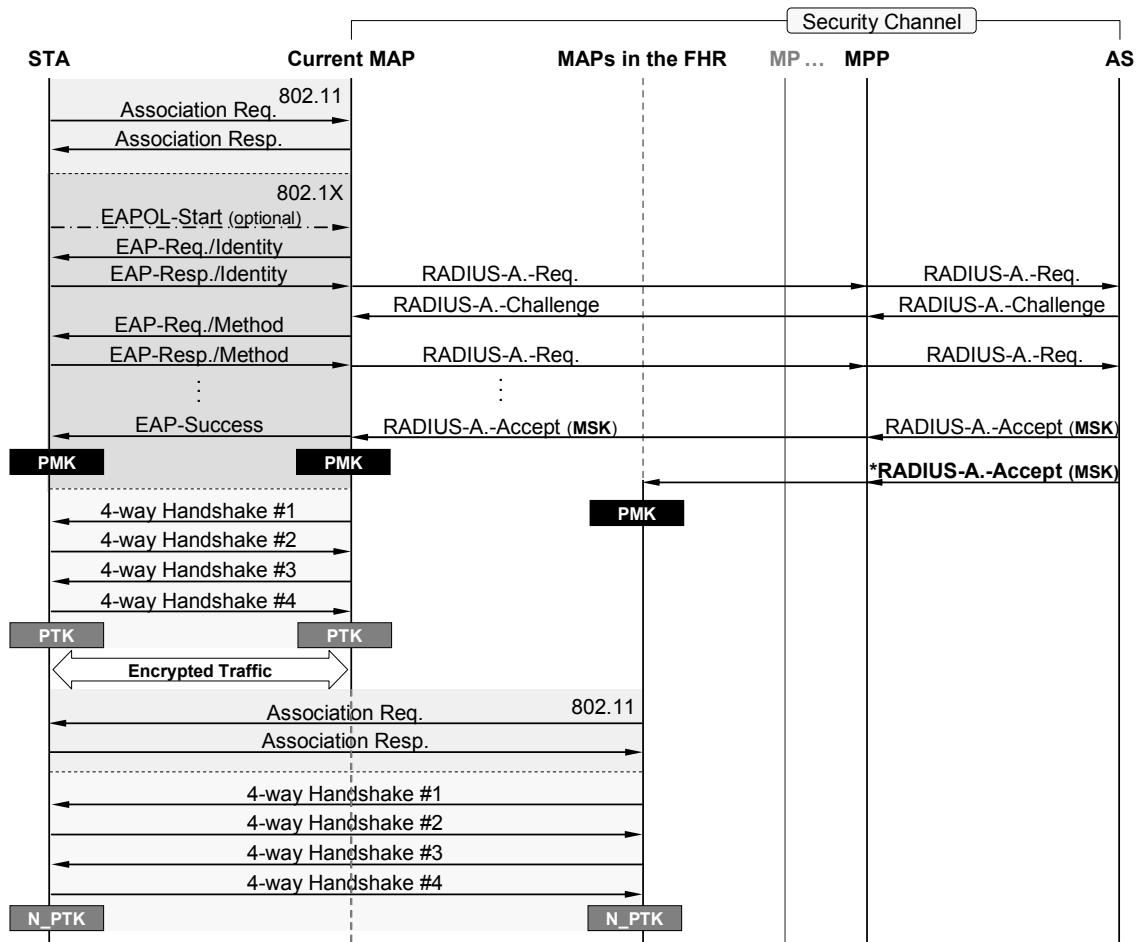


Figure 2-19 FHR scheme

The authentication procedures of FHR scheme are shown in Figure 2-19, where the messages with the star symbol are different with 802.1X. The message flows of FHR scheme are the same as 802.11i, except the MSK is distributed to multiple MAPs. The AS proactively distributes the MSK to APs in the FHR, and thus the target AP can derive the PMK before the handoff.

The negative effect of FHR scheme includes not only the overhead of AS for maintaining FHR and monitoring the location of STAs, but also violating the key management policy<sup>3</sup> and the trust relationship of the EAP protocol.

### 2.5.3 PMK Predistribution

With PMK predistribution mechanisms, a new PMK is derived and distributed to candidate APs in advance of the handoff. Due to a PMK can only be derived from an MSK obtained from the EAP method, a new key hierarchy has to be introduced to 802.11i. The key representing that an STA is authenticated and the key representing the permission to access the network are separated. Some advanced MAC layer protocols, such as IEEE 802.16e, adopts this concept, too.

The key separation not only reduces the authentication overhead but also limits the impact of the compromised PMK in a single AP. PMK predistribution mechanisms do not introduce new security vulnerabilities beyond the 802.11i standard, except the weakness of the key distribution. However, new key hierarchies are not compatible with current wireless devices. In practice, to update or replace all devices will be an arduous problem.

#### 2.5.3.1 Neighbor Graph Algorithm

A proactive key distribution scheme [16] proposed by Mishra et al. introduces a recur-

---

<sup>3</sup> An MSK is never exposed to any other party except the AS, the authenticator and the supplicant.



sive PMK derivation function, where

$$PMK_n = \text{TLS-PRF}(MSK, PMK_{n-1} | AP\_MAC | STA\_MAC) \quad (3)$$

The  $PMK_0$  is generated by the original key derivation function of 802.11i. A distinct  $PMK_n$  is distributed from AS to each adjacent APs of the associated AP respectively before the handoff, and thus the authentication phase are estimated.

To distribute PMK efficiently, AS maintains a data structure named neighbor graph (NG) to determine the set of candidate APs. The neighbor graph integrates the geographic information and is able to provide the accurate list of APs that an STA could potentially reassociate with.

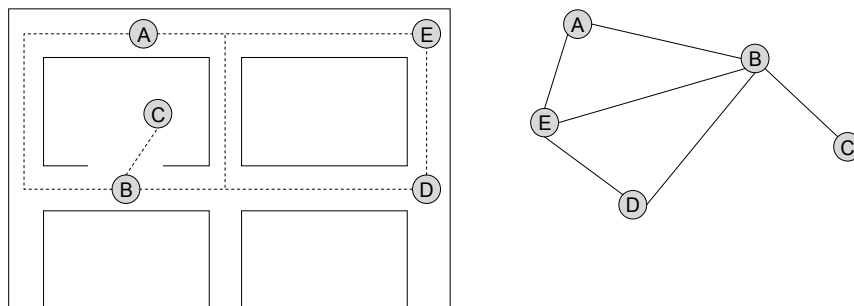


Figure 2-20 AP placement and the corresponding neighbor graph

An example of the AP placement is shown in Figure 2-20. The dotted line represents a potential path for the movement of STAs. If two APs are connected by a dotted line, there will be an edge between the  $AP_i$  and the  $AP_j$  in the neighbor graph, which is represented the handoff relationship.

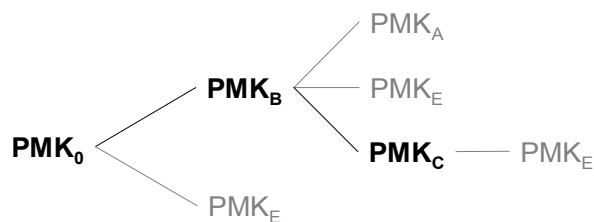


Figure 2-21 PMK derivations of the neighbor graph algorithm

Take an STA moving from A to C via B for example, the PMK derivations are shown as Figure 2-21. Note that if an AP appears in the candidate set repeatedly, the key duplication problem will happen, e.g. PMK<sub>E</sub>. This will result in the extra storage cost and the synchronization problem.

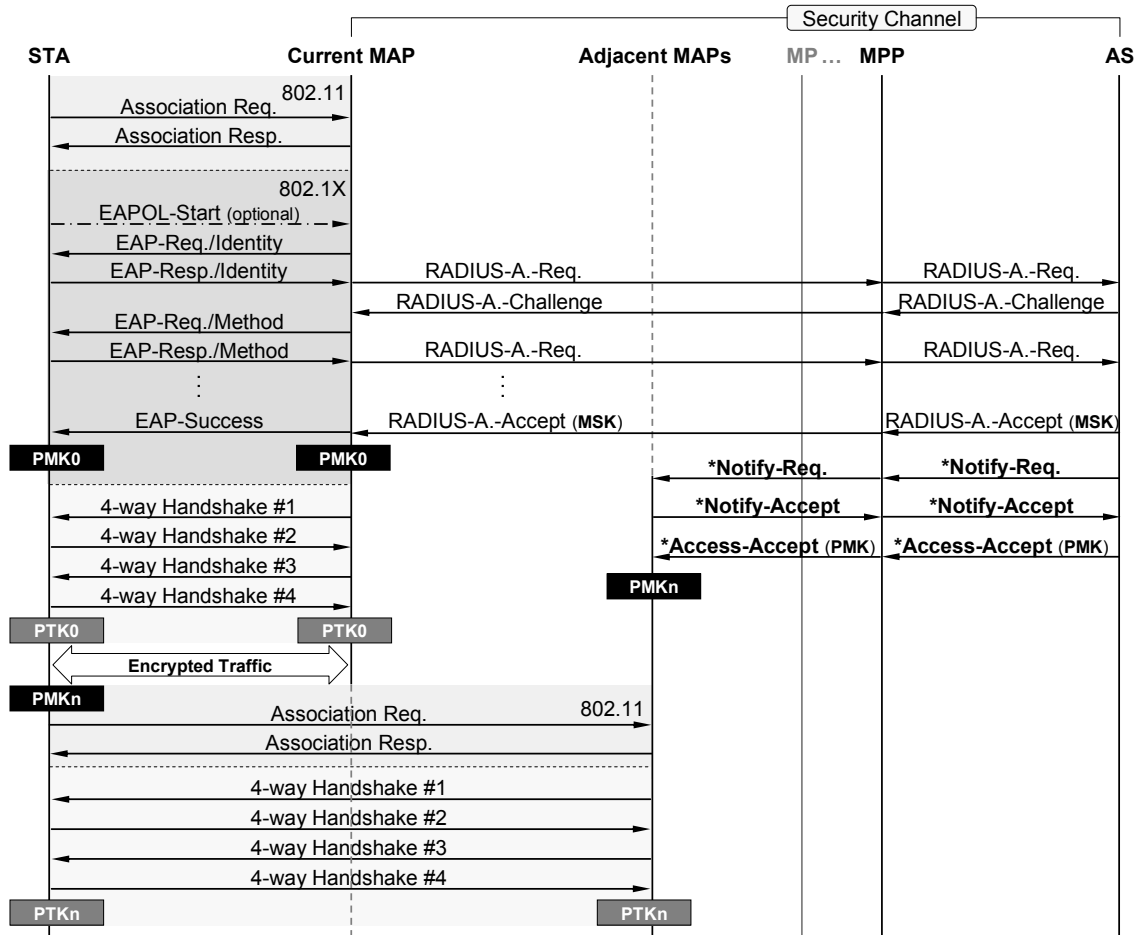


Figure 2-22 Neighbor graph algorithm

Figure 2-22 illustrates the message flows of NG scheme. If an STA passed the initial 802.1X authentication, the AS will send a Notify-Request message to the adjacent MAPs of the current MAPs to inform that the STA may handoff to. The adjacent MAPs either reply a Notify-Accept message to request the PMK<sub>n</sub> or a Notify-Reject message to bypass the PMK redistribution.

The disadvantage of NG scheme is the burden of AS for tracking the location of STAs and requiring multiple PMK derivations and distributions for each handoff.

### 2.5.3.2 Fast BSS Transition

802.11r [13] proposed a mechanism to minimize the handoff latency during the BSS transition. The fast BSS transition mechanism permits an STA to establish link security with the target AP prior to or during the commit phase, and thus avoids the delay in connecting to the DS after the handoff. The security improvements of 802.11r include:

1. Define a set of APs named mobility domain (MD). Once an STA passed the 802.1X authentication in any AP within the MD, the subsequent authentications can be skipped while the STA reassociates with other APs within the same MD.
2. Enhance the commit phase by introducing the fast transition authentication sequences to aggregate frames exchanged in the 4-way handshake into the link layer authentication/association frames.

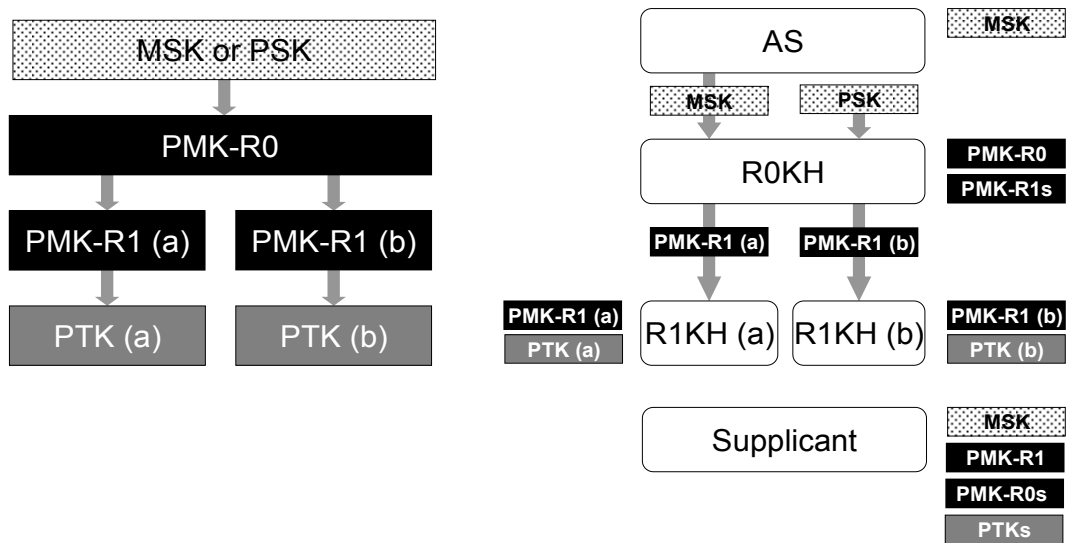


Figure 2-23 Key hierarchy and derivations of 802.11r

As shown in Figure 2-23, a new key hierarchy and two types of the key holder are introduced by 802.11r. The functions of 802.1X authenticator are distributed among a PMK-R0 key holder (R0KH) and PMK-R1 key holders (R1KHs). The R0KH derives a PMK-R1 from the PMK-R0 for each PMK-R1 key holder (R1KH) within the MD. The

R1KH derives the PTK mutually with the STA through the 4-way handshake.

As shown in Figure 2-24, the STA performs the initial fast transition (FT) association while first entering the MD. After that, the R0KH, i.e. the current MAP, predistributes the PMK-R1 to the target MAP. The distribution protocol is not defined by 802.11r, but some implementations choose the IAPP CACHE-notify mechanism to distribute PMK-R1.

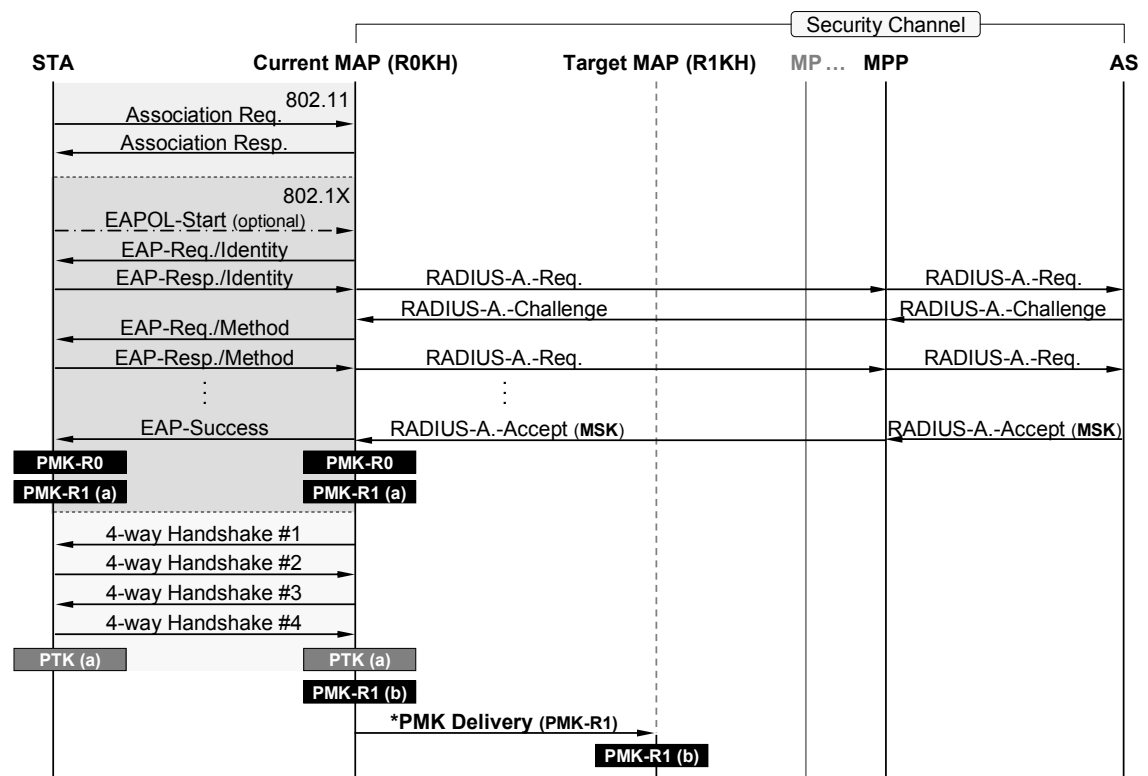


Figure 2-24 802.11r initial FT association and PMK-R1 predistribution

802.11r defines two mechanisms to improve the handoff performance. The authentication information exchanged between STA and target AP is either directly transmitted over the air in the commit phase (referred to as the Over-the-Air) or forwarded via the current AP before the handoff (referred to as the Over-the-DS).

The procedures of Over-the-Air fast BSS transition are shown in Figure 2-25. The FT authentication allows a fresh PTK to be computed in the commit phase, and thus authentication phase and handshake phase of are removed.

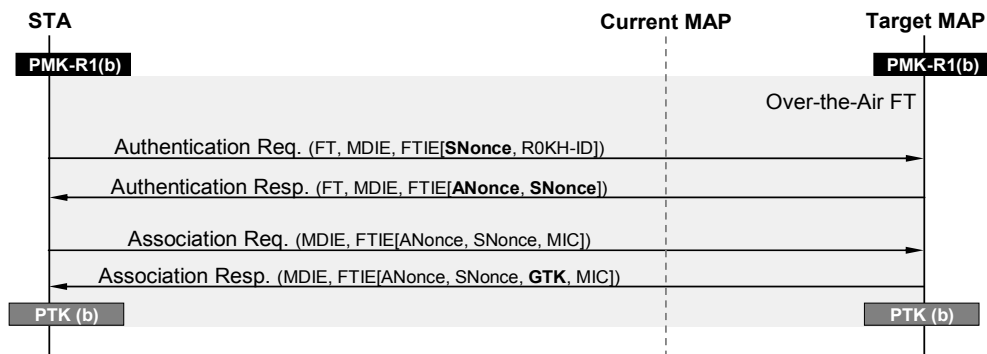


Figure 2-25 Over-the-Air FT authentication

The procedures of Over-the-Ds fast BSS transition are shown in Figure 2-26. FT Action frames carried the authentication information are forwarded between the STA and the target MAP via the current MAP. The MAC address of the target MAP is specified in the FT Action Request frame to indicate the forwarding destination.

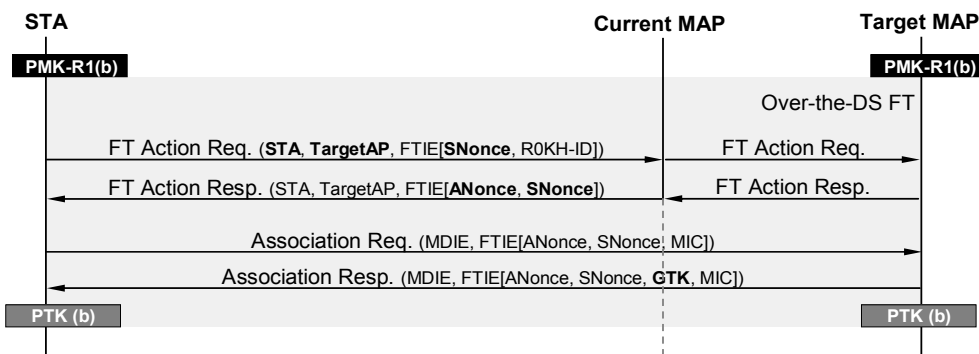


Figure 2-26 Over-the-DS FT authentication

The Over-the-DS mechanism minimizes the message exchanges for an STA to regain the connectivity, and thus the handoff latency can be significantly reduced.

However, fast BSS transition mechanism needs to determine the candidate APs for the PMK-R1 predistribution. If the prediction is missing, target MAP will have to retrieve the PMK-R1 from R0KH after the handoff, and it will cause extra latency. Moreover, the message aggregation for 4-way handshake will certainly increase the latency of the original commit phase.

## 2.5.4 Summary

The design of 802.11i, such as key hierarchy and redundant open system authentication, does not take the handoff into consideration and affects the quality of time-sensitive applications. Furthermore, most EAP methods require multiple round-trip message exchanges and will result in significant authentication latency.

Since 802.11 is a link layer protocol, it should not touch the problem out of the scope, i.e. EAP authentication latency. Related researches focus on reducing the demand of the EAP authentication instead of improving it.

802.11r provides a solution to optimize message exchanges and separate the 802.1X authentication from the network access control. However, considerable quantities of conventional WLANs have been deployed. These devices support neither the fast authentication nor the target AP prediction. It is impossible to replace or update all devices in the near future.

Besides, the 802.11 handoff is a mobile controlled handoff (MCHO), while the handoff decision is decided by the STA. Since STAs are powered by the battery, the handoff algorithms must consider the power consumption of the signal measuring and analysis. Some mechanisms, such as the NG scheme, can provide the precisely target AP prediction but require the topology information to assist the decision.

We propose a new security mechanism for STAs to remove the authentication phase from handoff procedures. The proposed mechanism performs on the premise that the security of 802.11i RSN is assured. Neither MSK nor PMK is transmitted via the wireless media. Furthermore, no modifications are needed for STAs to apply the new mechanism. The proposed mechanism is presented in the next chapter.

# Chapter 3

## Integrated Security Domain

To reduce the overhead of authentication and encryption processing, we propose a mechanism to integrate the security domains of WLAN Mesh. An MPP and the MAPs connected to this MPP form an integrated security domain (ISD). An STA only performs 802.1X authentication while first time connects to an MAP within the ISD. Authentication latency is removed from the following handoffs in the same ISD. Furthermore, an end-to-end security channel between an STA and an MPP is established without exchanging any extra message. The security channel can improve the performance of WLAN Mesh in routing the encrypted frame.

### 3.1 Architecture

With ISD, security functions of the AP services, such as 802.1X authentication and RSNA key management, are implemented in the MPP. As shown in Figure 3-1, the role of 802.1X authenticator is adopted by the MPP instead of the serving MAP.

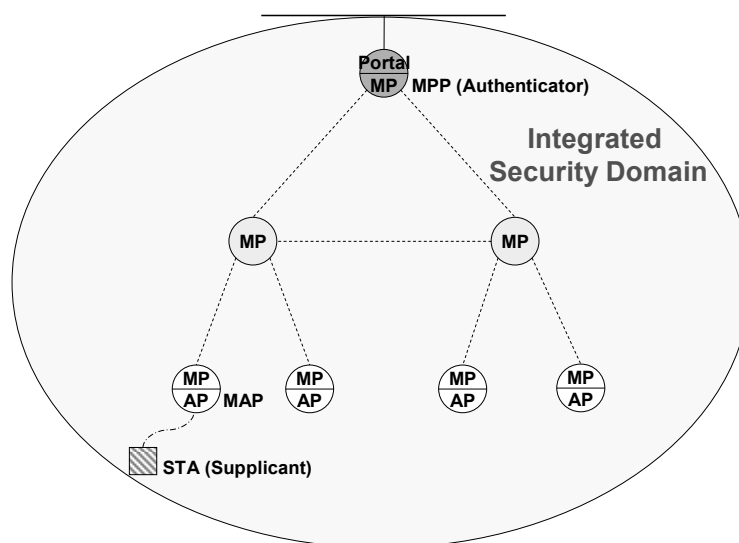


Figure 3-1 WLAN Mesh security architecture with ISD

MAP is the edge of WLAN Mesh and responsible for blocking malicious STAs from accessing the network. In order to provide the ability for MAP to verify frame integrity, PTK and GTK are distributed from MPP to the serving MAP via secured mesh links right after 4-way handshake. Figure 3-2 shows the PTK distribution.

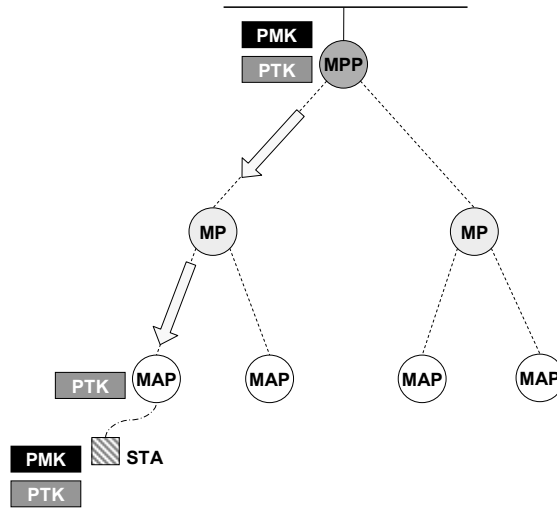


Figure 3-2 PTK distribution

### 3.2 RSNA Establishment

While an STA initially associated to any MAP within the IDS, it is required to perform 802.1X authentication and 4-way handshake to establish the security association with the MPP. For being compatible with conventional STAs, the message flows in the STA portion are identical to ISD and 802.11i in the RSNA establishment.

Since MPP is an authenticator, serving MAP participates in neither 802.1X authentication nor 4-way handshake but forwards all authentication messages between STA and MPP. Figure 3-3 illustrates the procedures of RSNA establishment for an STA initially authenticating with an MAP within the ISD.

1. The serving MAP checks the Association Request frame to see if any PMKID is included. If not, an STA Authentication Request message is sent to the MPP to initialize 802.1X authentication.



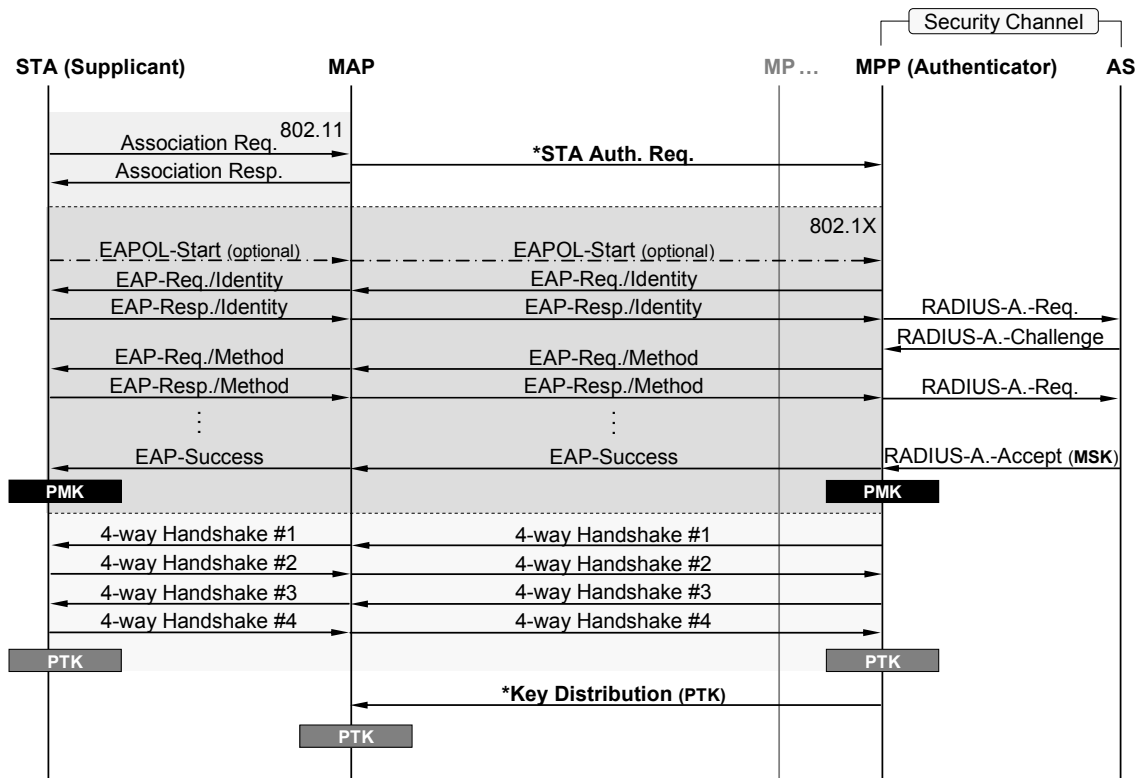


Figure 3-3 RSNA establishment with ISD

2. The STA and the MPP perform 802.1X authentication and 4-way handshake, and all messages are forwarded via the serving MAP.
3. The MPP distributes the PTK to the serving MAP for integrity verifying.
4. Once the serving MAP obtains the PTK, it will switch the port to the authorized state, and thus the STA is able to access the network.
5. If a GTK is assigned by the MPP in 4-way handshake, it will be distributed to the serving MAP as well.

### 3.3 Handoff Procedures

802.11s allows multiple MPPs reside in one WLAN Mesh, and thus the handoff behaviors with ISD are categorized into intra-MPP handoff and inter-MPP handoff. Moreover, the authentication procedures vary in the two types.

### 3.3.1 Intra-MPP Handoff

Intra-MPP handoff means that an STA drops current connection and reassociates with another MAP connecting to the same MPP.

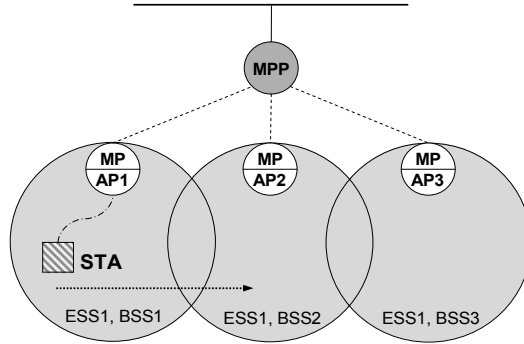


Figure 3-4 Intra-MPP handoff

Since MPP is the authenticator, STA does not change the authenticator in the intra-MPP handoff. If the PMK is cached by the authenticator, 802.1X authentication will be skipped. Figure 3-5 illustrates the message flows of intra-MPP handoff.

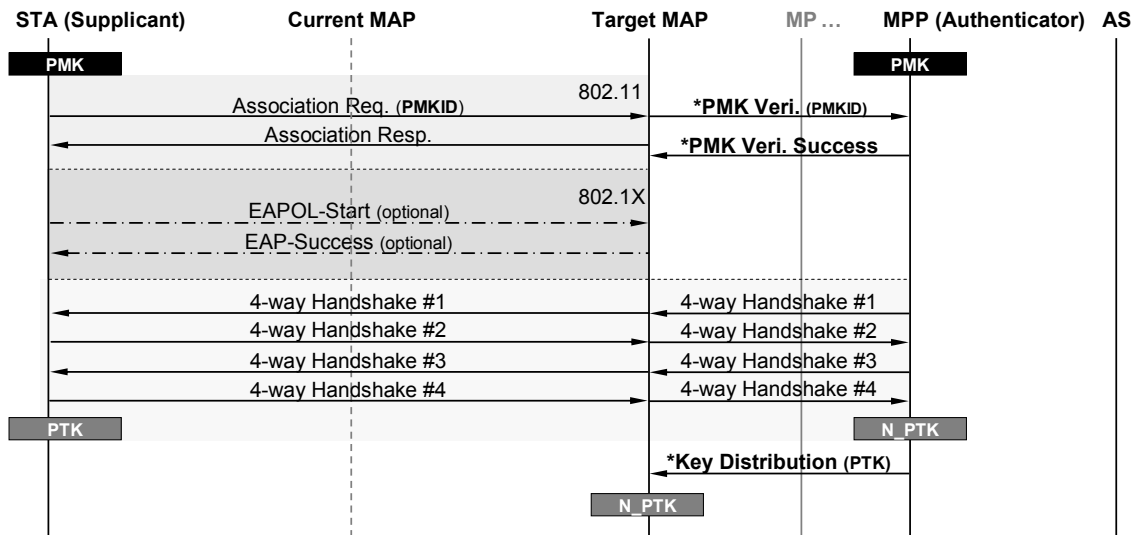


Figure 3-5 Intra-MPP handoff with ISD

1. The STA reassociates with the target MAP. The PMKID is passed to the MPP for verifying the PMK cached in the STA.
2. The PMKID is compared with the PMK cached in the MPP. If the PMKID is

valid, the MPP will inform the target MAP with a PMK Verification Success message.

3. Some implementations<sup>4</sup> of the supplicant use the EAPOL-Start message to initialize 802.1X authentication. If the target MAP receives an EAPOL-Start message, it will reply an EAP-Success message to skip the EAP authentication.
4. Following 4-way handshake and PTK distribution are identical to the RSNA establishment mentioned before.

### 3.3.2 Inter-MPP Handoff

Inter-MPP handoff is performed while an STA moves from one MAP to another MAP connecting to the different MPP. The STA will switch to another ISD in the inter-MPP handoff.

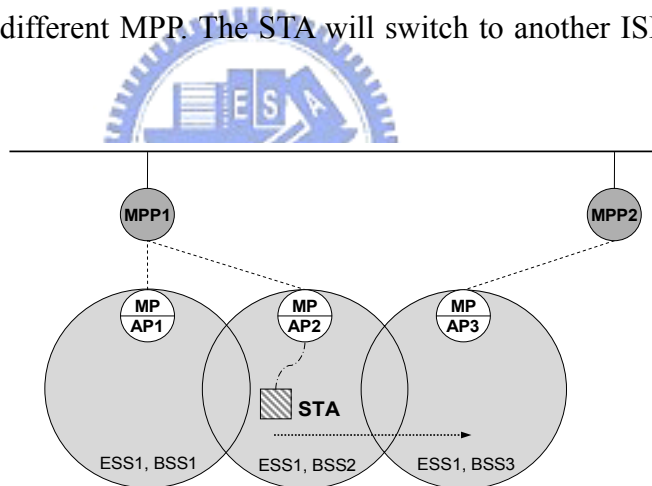


Figure 3-6 Inter-MPP handoff

If the ISD has not been visited by the STA or the cached PMK is expired, preauthentication will be performed. However, the STA may fail to preauthenticate with the new MPP, and thus the overhead of 802.1X authentication is introduced.

There are many factors cause preauthentication to be failed, such as the moving speed of the STA, the size of the overlapping coverage area, the target AP prediction,

---

<sup>4</sup>The EAPOL-Start message is used by Wireless Zero Configuration service in Windows XP, but not wpa\_supplicant 0.5.7 in Linux.

the latency of EAP authentication, etc.

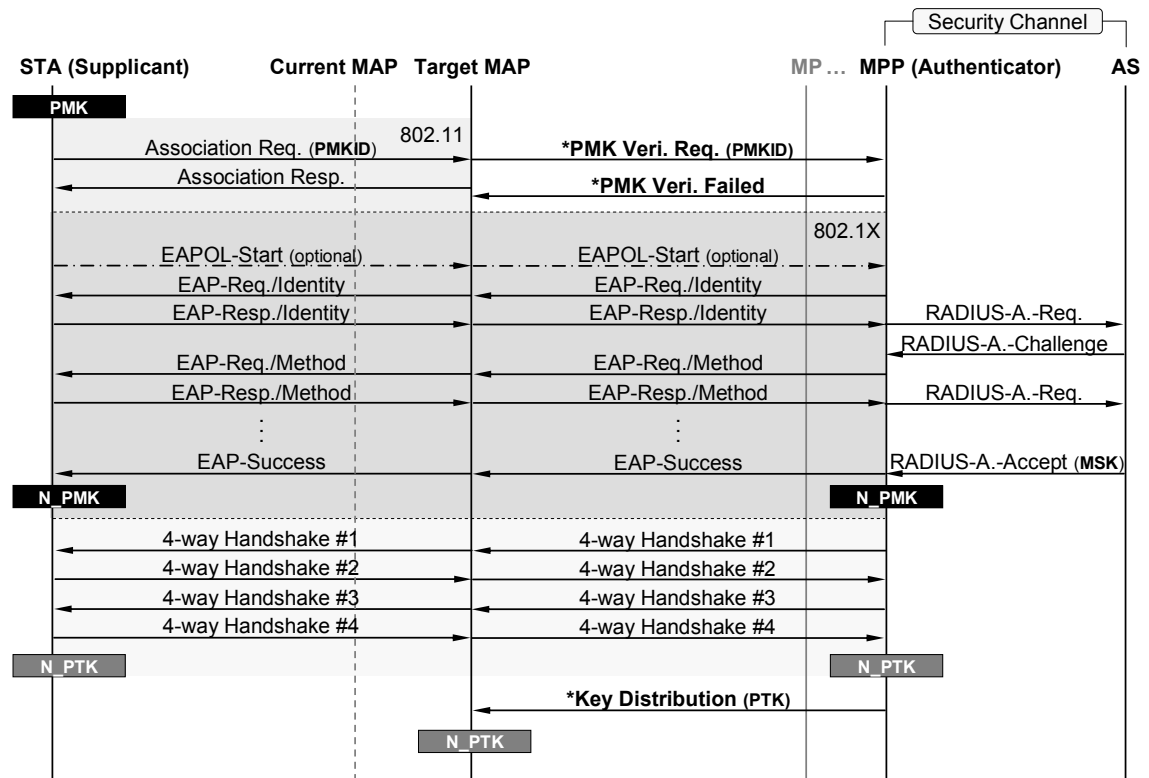


Figure 3-7 Inter-MPP handoff with ISD

Figure 3-7 illustrates the message flows of inter-MPP handoff and RSNA establishment. Detail procedures are as follows:

1. The STA reassociates with the target MAP. The PMKID is forwarded to the MPP for verifying the PMK cached in the STA.
2. Since the new MPP does not cache the PMK, the PMKID verification is failed, and a message will be sent to the target MAP for informing that following authentication messages should be forwarded to the MPP.
3. 802.1X authentication and 4-way handshake are performed, followed by the PTK distribution. The procedures are the same as the RSNA establishment described in section 3.2.

### 3.4 Encapsulation

To mitigate the routing overhead incurred by the hop-by-hop encryption in the

multi-hop network, the proposed mechanism establishes an end-to-end security channel between STA and MPP. Therefore, if the correspondent host is outside the WLAN Mesh, encryption and decryption operations will be only performed by serving MAP and MPP.

Encryption protocols of 802.11i, i.e. TKIP and CCMP, take some or all fields of the MAC header as inputs. As shown in Figure 3-8 and Figure 3-9, the inputs with the star symbol are referenced from the MAC header.

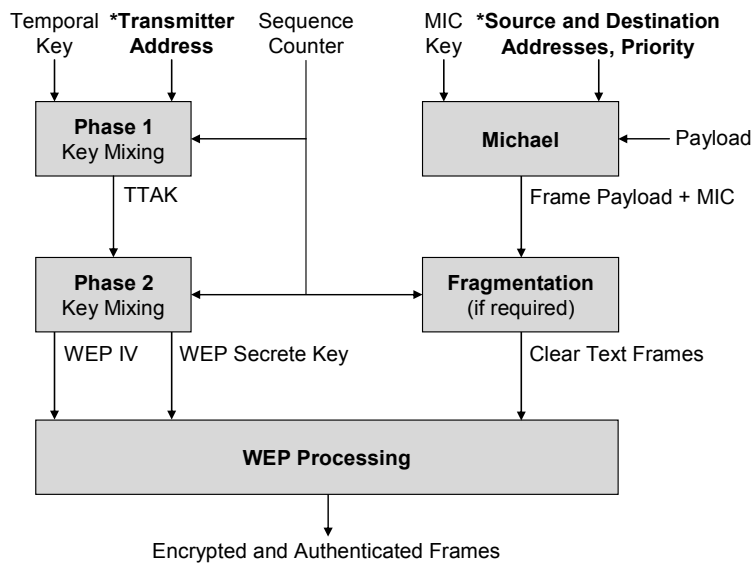


Figure 3-8 TKIP frame encryption processing

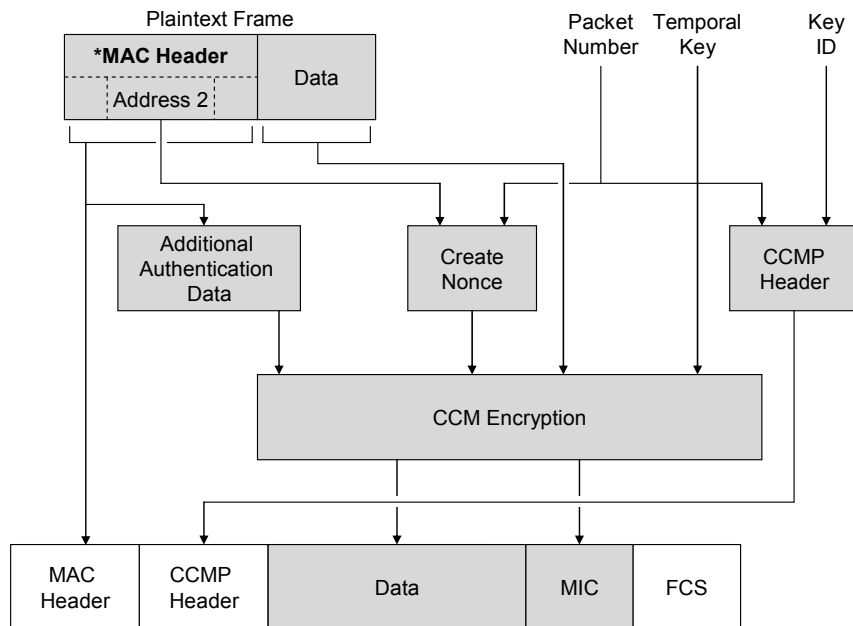


Figure 3-9 CCMP frame encryption processing

However, the MAC header generated by the source will be replaced in routing operations. Thus, one end of the security channel can not decrypt the frame encrypted by another end.

We construct a bidirectional MAC tunnel between serving MAP and MPP to avoid the MAC header used as the input of the frame encryption processing being modified.

Figure 3-10 gives an instance to explain the encapsulation processing of ISD.

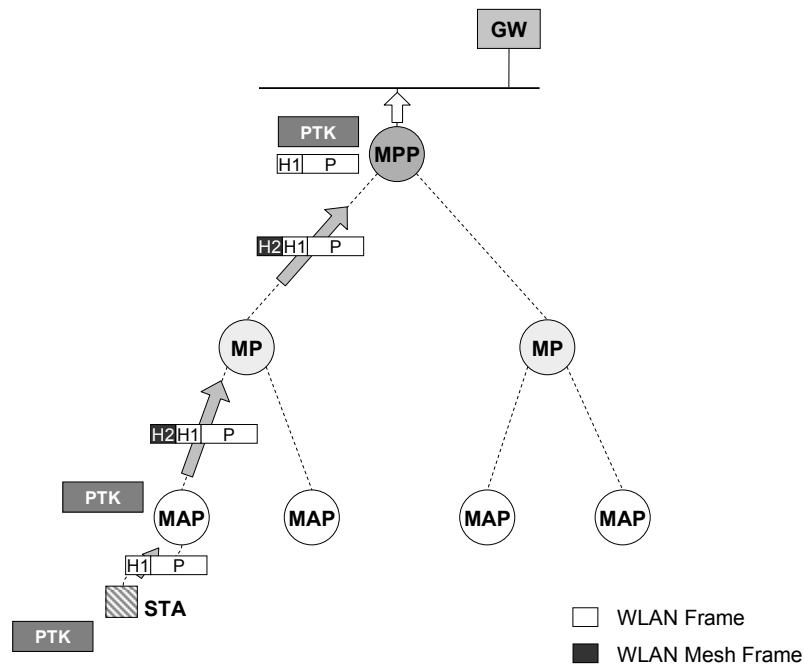


Figure 3-10 Encapsulation processing (external destination)

The STA transmits a WLAN frame to the destination which is outside the WLAN Mesh, e.g., the default gateway (GW). Detail procedures are as follows:

1. The STA constructs a WLAN frame (H1 + P, where H1 is the header of the WLAN frame, and P is the payload) and encrypts the frame with the PTK.
2. The WLAN frame is transmitted to the serving MAP via an 802.11 link.
3. The MAP verifies the MIC code of the frame with the PTK. If the MIC code is invalid, this frame will be discarded, otherwise the destination will be examined.
4. If the destination is outside the WLAN Mesh, the MAP will encapsulate the

WLAN frame into a WLAN Mesh frame (H2 + H1 + P, where H2 is the header of the WLAN Mesh frame) and forward the frame to the next hop. Thus, the inner header (H1) will not be altered in the routing.

5. The MP forwards the frame to the next hop. No further operations are needed.
6. The MPP removes the WLAN Mesh header (H2) and decrypts the WLAN frame (H1 + P) with the PTK.
7. Finally, the MPP encapsulates the payload (P) into an Ethernet frame and forwards the frame to the destination.

Figure 3-11 illustrates the encapsulation processing for the source which is outside the WLAN Mesh. For example, the GW transmits an Ethernet frame to the STA.

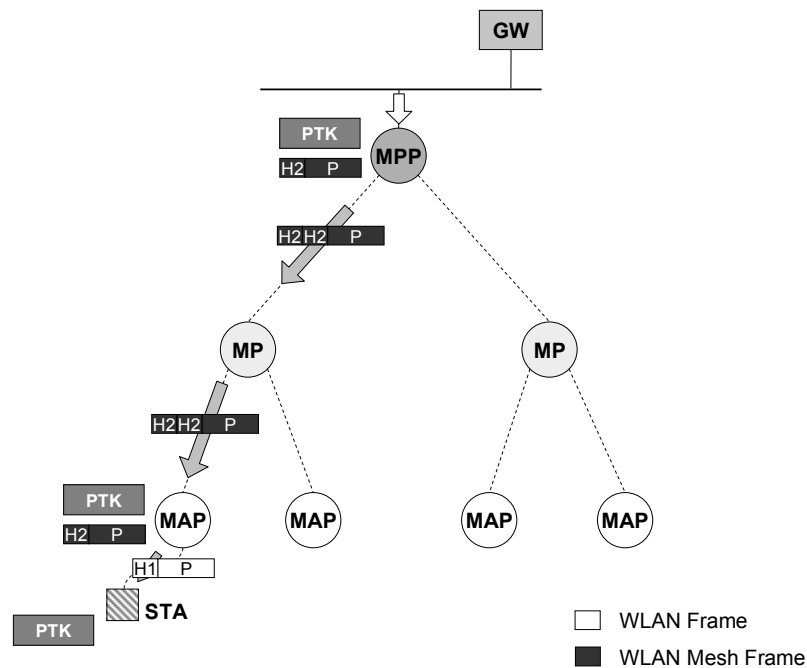


Figure 3-11 Encapsulation processing (external source)

1. The MPP receives an Ethernet frame and translates into the WLAN Mesh format (H2 + P). The frame is encrypted by the PTK and encapsulated into another WLAN Mesh Frame (H2 + H2 + P). Two identical WLAN Mesh headers can keep the inner header intact in the routing. After encryption and encapsulation processing finished, the MPP forwards the frame to the next

hop.

2. The MP forwards the frame to the next hop.
3. The MAP removes the outer WLAN Mesh header (H2) and decrypts the inner WLAN Mesh frame (H2 + P) with the PTK.
4. The MAP encapsulates the payload (P) into a WLAN frame (H1 + P) and encrypts the frame with the PTK. Finally, the MAP forwards the WLAN frame to the STA.

To improve the routing performance, if destination and source are both reside the WLAN Mesh, 802.11s will apply the shortcut routing path instead of the regular routing path while. For example, as shown in Figure 3-12, D→B→A→C→G is replaced by D→B→C→G.

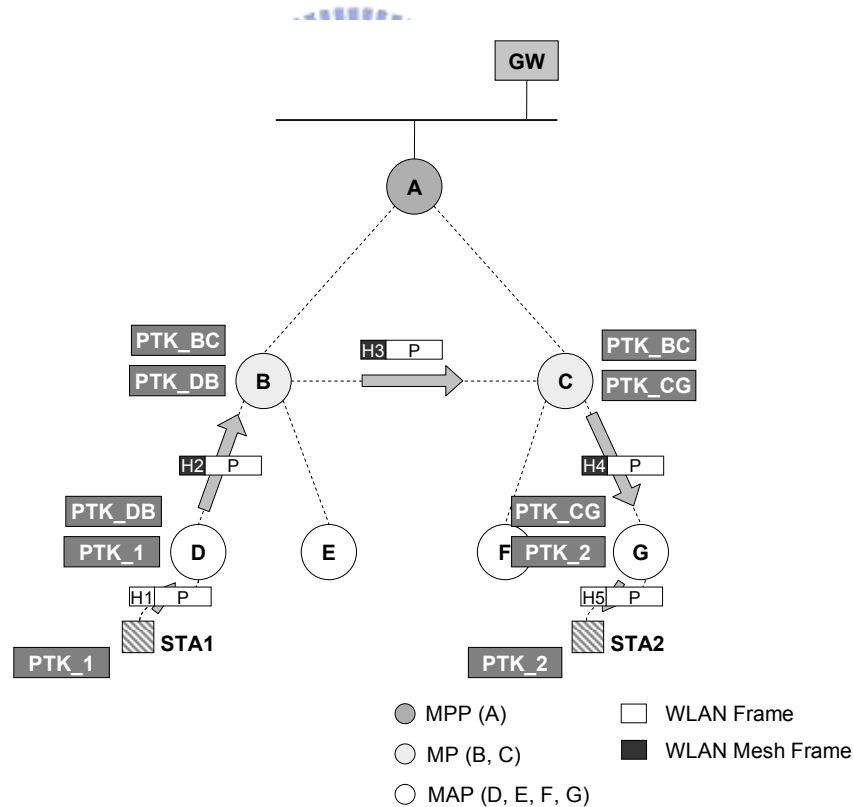


Figure 3-12 Encapsulation processing (internal)

To support the shortcut routing path, ISD applies the original hop-by-hop encryption of 802.11s. Figure 3-12 shows the encapsulation processing for the STA1 transmit-



ting a WLAN frame to the STA2. Detail procedures are as follows:

1. The STA1 constructs a WLAN frame (H1 + P). The frame is encrypted with the PTK\_1 and transmitted to the MAP D.
2. The MAP D decrypts the WLAN frame with the PTK\_1 and encapsulates the payload (P) into a WLAN Mesh frame (H2 + P). The frame is encrypted with the PTK\_DB and forwarded to the MP B.
3. The MP B and the MP C decrypt the frame and then re-encrypt it with the PTK of the next-hop. After that, the frame is forwarded to the next-hop.
4. The MAP G decrypts the WLAN Mesh frame with the PTK\_CG and encapsulates the payload (P) into a WLAN frame (H5 + P). The frame is encrypted with the PTK2 and forwarded to the STA2.
5. STA2 decrypts the WLAN frame with the PTK\_2.

### 3.5 Fragmentation Issue

The maximum transmission unit (MTU) defines the largest frame size that the link layer protocol can pass onwards. The encapsulation mechanism of ISD needs an additional WLAN Mesh header and could result in extra fragmentations.

The fragmentation issue can be avoided by configuring the MTU value of the mesh network. As showing in Figure 3-13 (a), modern operating systems, such as Window XP and Linux, treat the wireless NIC as an Ethernet NIC, and the default MTU value of the wireless NIC is 1500 bytes.

According to 802.11s, the size of a WLAN frame encapsulated into a WLAN Mesh frame is 1552 bytes. As shown in Figure 3-13 (b), since the allowable size of the largest encrypted frame is 2356 bytes (TKIP) or 2372 bytes (CCMP), there will be enough free space for the additional WLAN Mesh header. The administrator can set the MTU value of the mesh network to be 1552-2372/2376 to avoid the extra fragmentation.

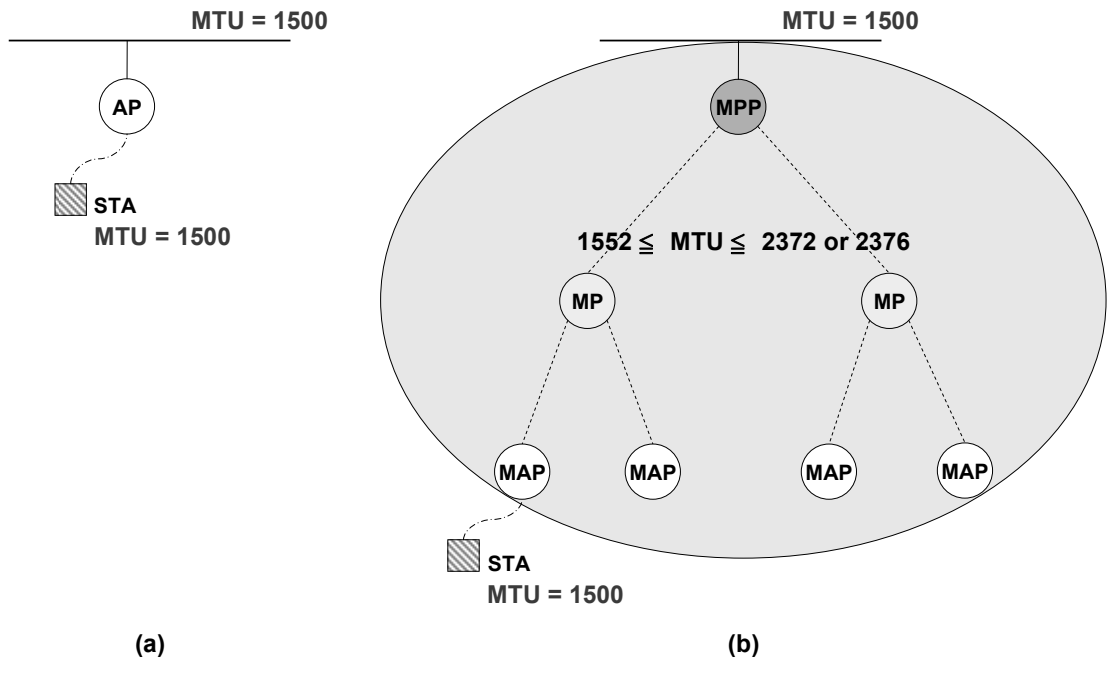


Figure 3-13 MTU value and fragmentation issue



# Chapter 4

## Security Considerations

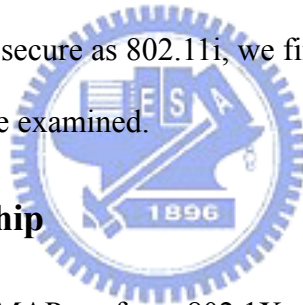
To claim that ISD is a secure mechanism, it is necessary to state the security goal as well as the security assumptions. The security goal of ISD is to secure the wireless communication between STA and MAP, and the strength of ISD should be equivalent to 802.11i.

ISD assumes that STAs and MAPs are 802.11i-based devices and the 802.11i security assumptions should be satisfied. Besides, mesh links among MPs are required to be protected by EMSA services.

To present ISD is as secure as 802.11i, we first analyze the trust relationship of ISD, and then threat models are examined.

### 4.1 Trust Relationship

An STA and its serving MAP perform 802.1X authentication and 4-way handshake to establish the RSNA in the ASD. Therefore, the STA $\leftrightarrow$ AS $\leftrightarrow$ MAP trust chain shown in Figure 4-1 is established by 802.11i. To secure the connection between STA and MAP, ISD must provide an equivalent STA $\leftrightarrow$ MAP trust relationship.



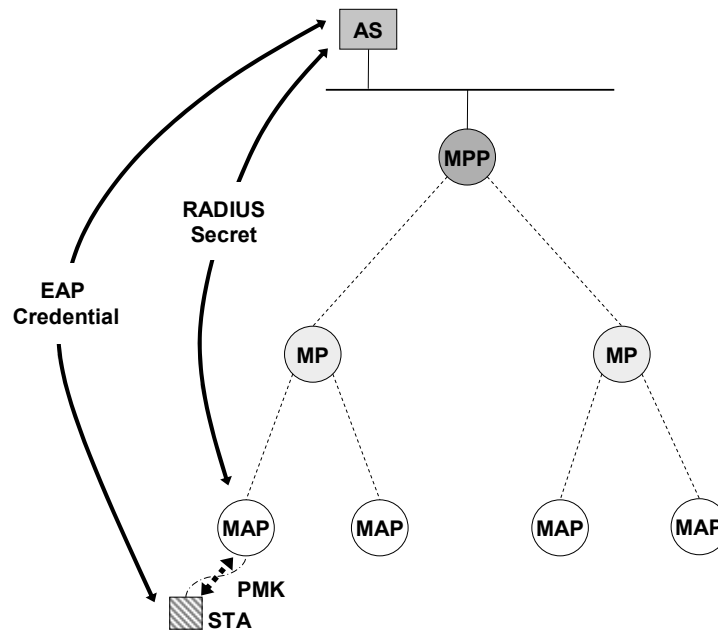


Figure 4-1 Trust Relationships in the ASD

As shown in Figure 4-2, mesh links between two MPs are secured by the EMSA, and thus there is an MAP↔AS↔MP↔AS↔...↔MPP trust chain established in the MSD.

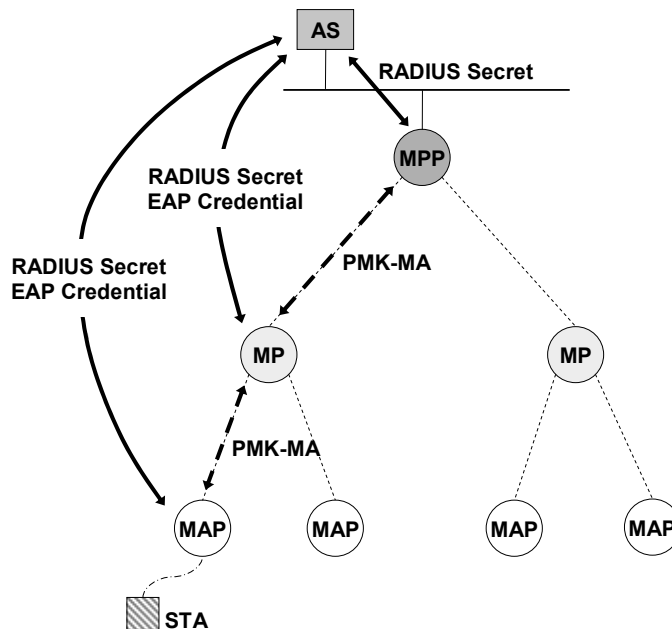


Figure 4-2 Trust Relationships in the MSD

For ISD, as shown in Figure 4-3, 802.1X authentication and 4-way handshake are performed by the STA and the MPP, and the STA↔AS↔MPP trust chain is established.

Since there is the MAP↔MPP trust relationship, the STA↔MPP↔MAP trust chain can be inferred from the former two trust relationships. Therefore, we can claim that the trust relationship provided by ISD is equivalent to 802.11i.

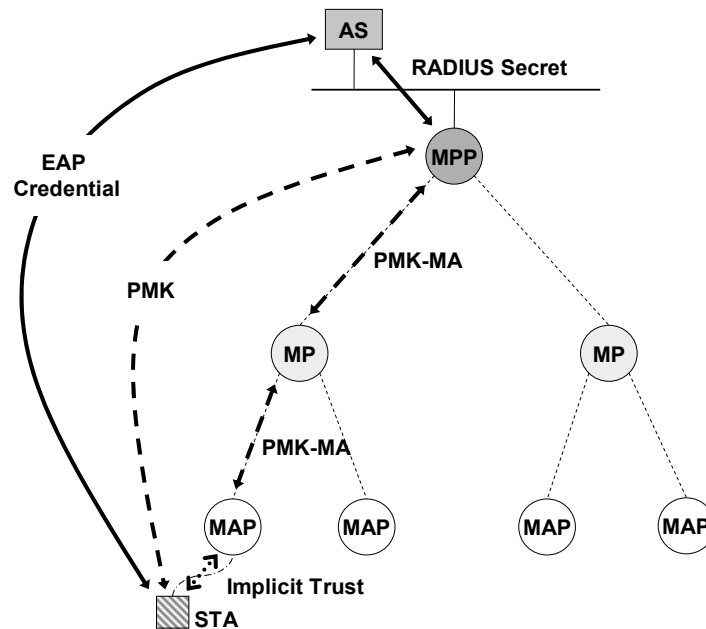


Figure 4-3 Trust Relationships in the ISD

In terms of the handoff, there are three related trust relationships: STA↔AS, STA↔MAP and STA↔MPP. The STA↔MAP trust relationship is destroyed in the intra-MPP handoff and needs to be reestablished. For ISD, since the STA↔MPP and the MAP↔MPP trust relationship are remained, the implicit trust exists between the STA and the new MAP. However, to secure the connection between the STA and the new MAP, a new PTK is necessary to prevent the unauthorized disclosure to the old MAP. Therefore, in the intra-MPP handoff, STA and MPP need to perform 4-way handshake to derive a fresh PTK. Since the old MAP has neither the new PTK nor the PMK, it can not obtain the content encrypted by the new PTK.

For 802.11i, to reestablish the STA↔MAP trust relationship, the STA needs to perform 802.1X authentication with the new MAP. Consequentially, it will introduce significant latency.

## 4.2 Threat Model

The proposed mechanism should avoid introducing any security degradation to the 802.11i RSN. In addition to the threats against 802.11i and 802.11s, there are other threats need to be recognized for ISD.

- **PMKID Leakage**

Even though an attacker may obtain the corresponding PMKID from previous eavesdropping and is able to skip 802.1X authentication, it does not result in any security flaw. Due to MSK and PSK are never transmitted via the wireless media, a valid PTK can not be derived by the attacker. Therefore, the attacker can not compute the valid MIC code of message #2 in the 4-way handshake, and the attacker is blocked by the MAP.

- **Authenticator Compromise**

In the situation that an authenticator is compromised or stolen, an attacker may obtain all PMKs cached in this authenticator. With ISD, the attacker can access the WLAN Mesh via any MAP connected to this authenticator. However, 802.11r also incurs this vulnerability. The compromised authenticator in 802.11r will expose PMK-R0s to the attacker. Since IEEE 802.11 working group allows this situation to occur, we believe this vulnerability is acceptable.

- **Unauthorized Disclosure**

Compromised mesh links will result in the unauthorized disclosure of keys. For 802.11i, an MSK is transmitted from the AS to the serving MAP via mesh links. If the security of mesh links is compromised, it is possible that the MSK will be exposed to an attacker. For ISD, only the PTK is transmitted via mesh links. Since the hierarchy of PTK is lower than MSK, the compromised PTK will not introduce further security degradation compared with the compromised MSK.

### 4.3 Advantages

With separated security domains, maintaining the consistent security configuration throughout the entire set of MAPs in the WLAN Mesh is problematic. Moreover, MAPs outside of the network center are difficult to apply the physical security control.

The proposed mechanism takes advantages of the centralized authenticator. It is much efficient to enforce security policy and distribute security configuration among the whole network in the centralized architecture. Furthermore, it is easier to enhance the physical security of one MPP instead of all MAPs within the WLAN Mesh.



# Chapter 5

## Handoff Overhead Estimation

In this chapter, we analysis the link layer security mechanisms and present the related handoff overhead. For STA, the major concern is whether the handoff latency will damage the quality of real-time applications or not. For WLAN Mesh, the handoff traf- fic is the main issue.

An analytical model is proposed to compute the handoff overhead for an STA roaming within the WLAN Mesh. The estimated handoff overhead of ISD and 802.11i will be compared in the end.

### 5.1 Handoff Model

In order to increase the channel capacity and reduce the transmission power, cell struc- ture shown in Figure 5-1 is adopted in most AP deployments, where each AP has 6 ad- jacent APs.

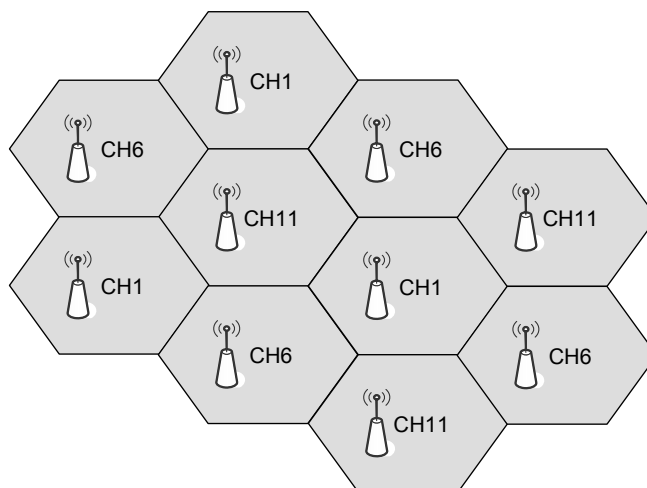


Figure 5-1 AP deployment based on the cell structure

In addition to the AP interface, an MAP has one or more MP interfaces to inter-



connect with other MPs. The topology of MP services may be different to AP services. An example of the MP topology is shown in the Figure 5-2, where the MAP deployment is based on the cell structure.

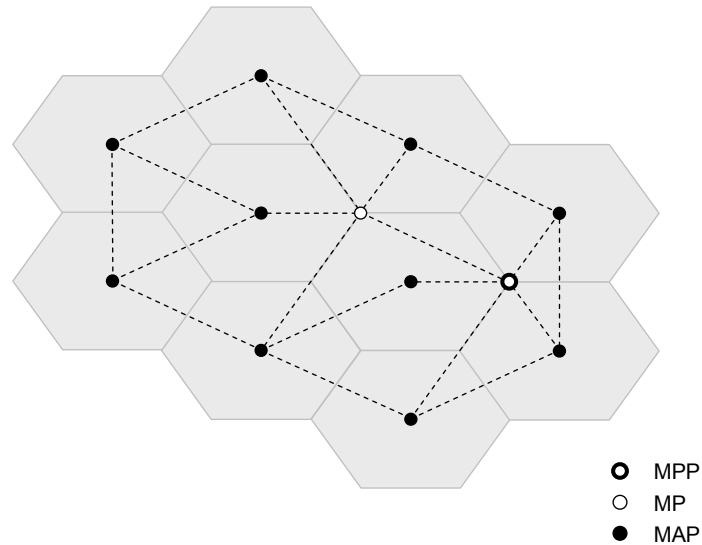


Figure 5-2 Topology of MP services

During the 802.1X authentication, RADIUS messages are forwarded between the serving MAP and MPP. Despite there are different WLAN Mesh topologies, only the hop count between MAP and MPP is related to the authentication latency and traffic. Therefore, we can conclude that the AP deployment determines the handoff behavior of STAs, and the MP topology determines the hop count between MAP and MPP. To estimate the handoff overhead, the analytical model has to take both of them into considerations.

For the AP deployment, the two-dimensional random walk model [4] is applied to capture the movement of STAs in the WLAN Mesh and calculate the number of handoffs. Figure 5-3 illustrates a 6-subarea cluster, where cells are marked as  $(x, y)$ . The  $x$  represents the layer of the cluster in which the cell resides, and  $y$  denotes the type  $y$ . Cells with the same set of neighbors' type are classified into one type. STAs in cells with the same type will have the same candidate handoff targets and will leave the cells with the same pattern. Therefore, the gray area shown in Figure 5-3 can capture the

movement of STAs within the cluster.

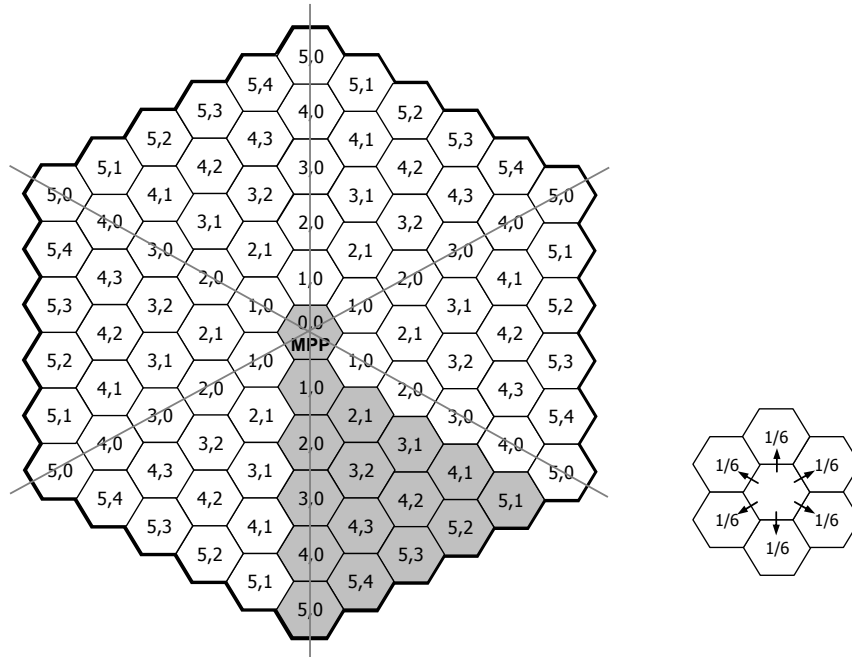


Figure 5-3 MAP deployment and cell classification

Assumptions of the handoff model are as follows:

- i. An STA resides in a cell and then moves to one of its neighbors with the equal probability, i.e.,  $1/6$ .
- ii. The cell (0, 0) is an MPP, and other cells are MAPs connected to this MPP. The MPP is also capable of providing the AP services.
- iii. The transmission distance of the MP interface is twice as long as the AP interface, which means the frame transmitted from MAP to MPP at least need  $x$  hops, and vice versa.
- iv. There are no such MPs which only participate in the backhaul routing. Based on assumptions iii and iv, Figure 5-4 illustrates the MP topology of the 3-subarea cluster. Despite there might be MP topologies violating assumptions iii and iv, only the average hop between MAP and MPP correlates the handoff latency and traffic.

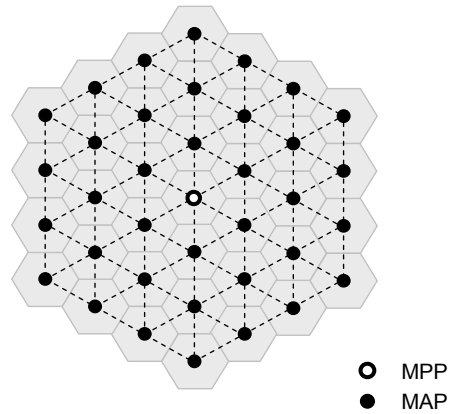


Figure 5-4 MP topology of the 3-subarea cluster

- v. The cached PMKs are never expired.<sup>5</sup>
- vi. For 802.11i, if the target MAP does not cache the PMK, STA needs to perform full 802.1X authentication to regain the connectivity.
- vii. For ISD, STA only needs to perform 4-way handshake in the handoff while roaming within the cluster.
- viii. For ISD, if the target MAP does not cache the PMK, STA needs to perform full 802.1X authentication while moving out of the cluster.

Based on the random walk theory, the random walk for an  $n$ -subarea cluster (e.g.  $n = 6$ ) can be converted into a state diagram shown in Figure 5-5.

---

<sup>5</sup> Windows XP specifies that the PMK cache can exist for 12 hours before being removed.

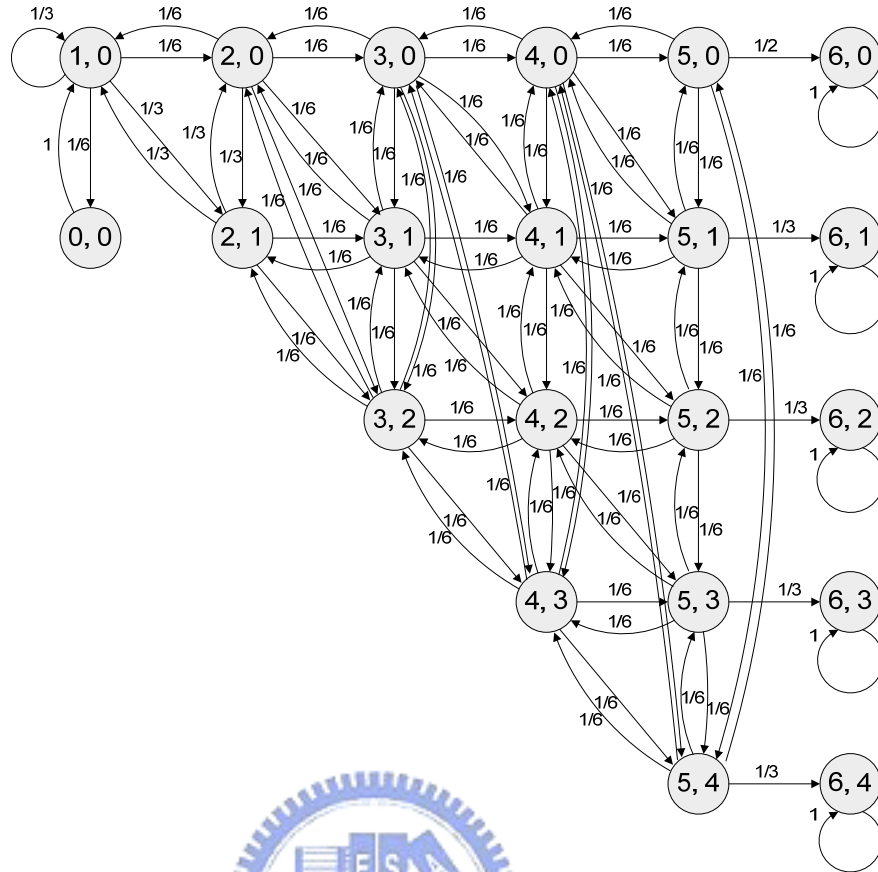


Figure 5-5 State diagram for a 6-subarea cluster

In this diagram, state  $(x, y)$  represents that an STA resides in one of the cells with type  $(x, y)$ , and state  $(n, j)$  means the STA moves out of the cluster from one of the cells  $(n-1, j)$ .  $S(n)$  represents the total numbers of states of the  $n$ -subarea cluster.

$$S(n) = \begin{cases} 2, & n = 1 \\ \frac{n(n+1)}{2}, & n > 1 \end{cases} \quad (4)$$

Let  $P_{(x,y),(x',y')}$  be the one-step transition probability from the state  $(x, y)$  to the state  $(x', y')$ , i.e., the STA performs one handoff from the current MAP  $(x, y)$  to the target MAP  $(x', y')$ . For a  $n$ -subarea cluster random walk, the transition matrix  $P = (p_{(x,y),(x',y')})$  is a  $S(n) \times S(n)$  matrix, where

$$\mathbf{P} = \left\{ \begin{array}{ccccccc} 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 1/6 & 1/3 & 1/6 & 1/3 & \dots & 0 & 0 \\ 0 & 1/6 & 0 & 1/3 & \dots & 0 & 0 \\ 0 & 1/3 & 1/3 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 \end{array} \right\}_{S(n) \times S(n)} \quad (5)$$

Let  $\mathbf{P}^{(k)}$  be the probability for an STA moves from an MAP to another MAP with  $k$  handoffs, where

$$\mathbf{P}^{(k)} = \begin{cases} \mathbf{P}, & k = 1 \\ \mathbf{P} \times \mathbf{P}^{(k-1)}, & k > 1 \end{cases} \quad (6)$$

An element  $p_{(x,y), (x',y')}^{(k)}$  in  $\mathbf{P}^{(k)}$  is the probability that the random walk moves from state  $(x, y)$  to state  $(x', y')$  with  $k$  handoffs. Let  $p_{k, (x,y), (n,j)}$  be the probability that an STA initially resides at the MAP  $(x, y)$  and moves out of the cluster at the  $k$ th handoff, where

$$p_{k, (x,y), (n,j)} = \begin{cases} p_{(x,y), (n,j)}, & k = 1 \\ p_{(x,y), (n,j)}^{(k)} - p_{(x,y), (n,j)}^{(k-1)}, & k > 1 \end{cases} \quad (7)$$

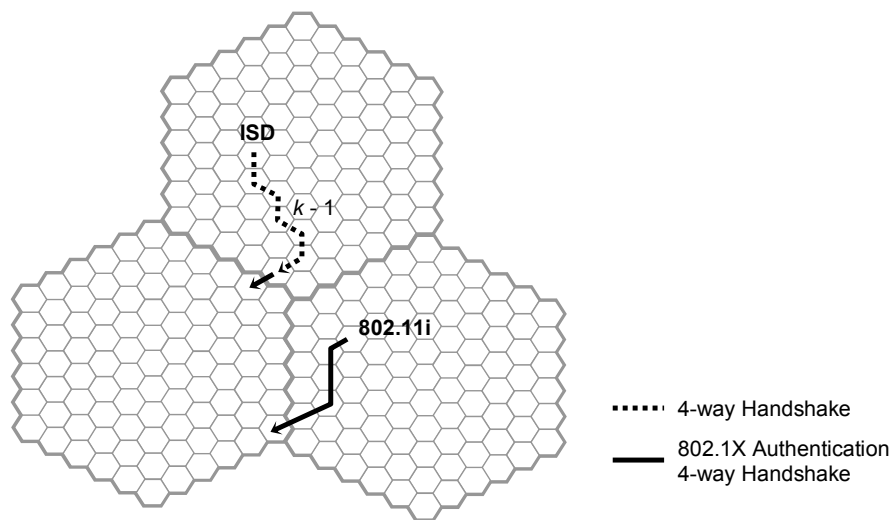


Figure 5-6 Handoff pattern for ISD and 802.11i

As shown in Figure 5-6, an STA moves out of the cluster at the  $k$ th handoff means that it performed  $k-1$  intra-MPP handoffs and one inter-MPP handoff. For ISD, an STA only performs 802.1X authentication in the inter-MPP handoff. However, for 802.11i, if the PMK is not cached by the target MAP, 802.1X authentication will be performed in the handoff.

## 5.2 Estimation Equations

To evaluate the link layer security mechanisms, we propose the equations to model the handoff overhead. With the handoff pattern, the proposed equations can estimate the average handoff latency and traffic for an STA roaming within the WLAN Mesh.

### 5.2.1 Handoff Latency

Whereas 802.1X authentication and 4-way handshake contribute the major part of the handoff latency, the quality of real-time applications is affected by the security mechanism. The latency introduced by the security mechanism can be classified into two types: intra-MPP handoff latency ( $L_{INTRA}$ ) and latency inter-MPP handoff latency ( $L_{INTER}$ ).

#### 5.2.1.1 Intra-MPP Handoff Latency

$L_{INTRA}$  represents the latency for an STA performing the intra-MPP handoff, which consists of authentication latency ( $L_{INTRA\_AUTH}$ ) and 4-way handshake latency ( $L_{INTRA\_4W}$ ).

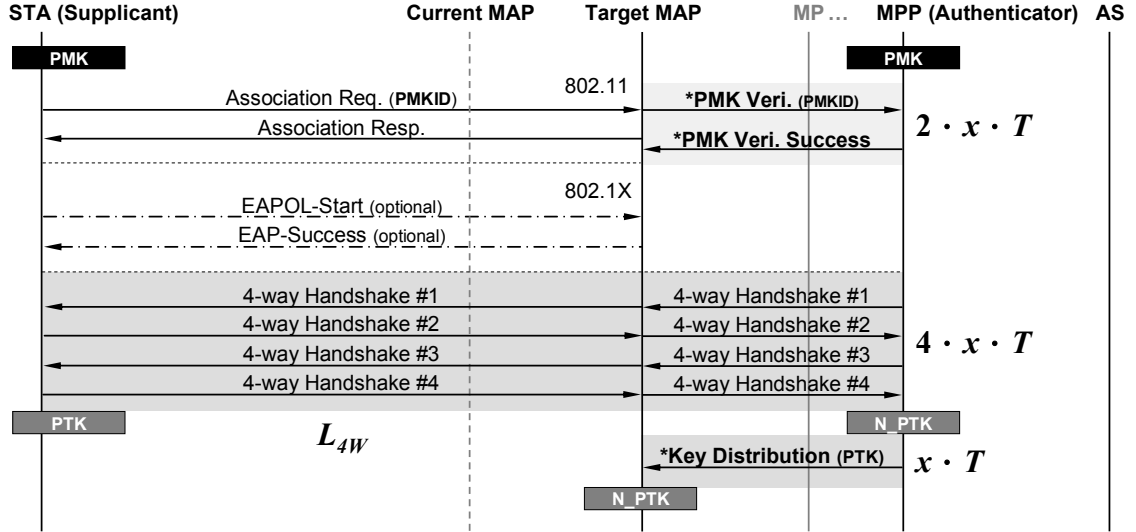


Figure 5-7 Intra-MPP handoff latency with ISD

For ISD, as shown in Figure 5-7, two messages are exchanged to verify the PMK cached by the STA.  $L_{INTRA\_AUTH}$  represents the average latency, where

$$L_{INTRA\_AUTH} = 2 \cdot T \cdot H, \quad \text{ISD} \quad (8)$$

$$H = \frac{\sum_{x=0}^{n-1} (x \cdot S)}{1 + n(n-1)/2} \quad (9)$$

$$S = \begin{cases} 1, & x = 0 \\ x, & x > 1 \end{cases} \quad (10)$$

- $T$  is the single-hop transmission time.
- $H$  is the average hop count between MAP and MPP.
- $\frac{\sum_{x=0}^{n-1} (x \cdot S)}{1 + n(n-1)/2}$  is calculated based on the proposed handoff model.
- $x$  is the hop count between MAP and MPP, i.e. the type of MAP.
- $S$  is the number of MAPs in the gray area with  $x$  hops to MPP.
- $n$  is the cluster size.  $1+n(n-1)/2$  is the total number of MAPs in the gray area.

In the handshake phase, 4-way handshake messages are transmitted between the STA and the MPP. In addition, the PTK is distributed to the target MAP.  $L_{INTRA\_4W}$

represents the average latency, where

$$L_{INTRA\_4W} = L_{4W} + 5 \cdot T \cdot H, \quad \text{ISD} \quad (11)$$

- $L_{4W}$  is the latency for an STA performing 4-way handshake in the single-hop network, i.e., WLAN.

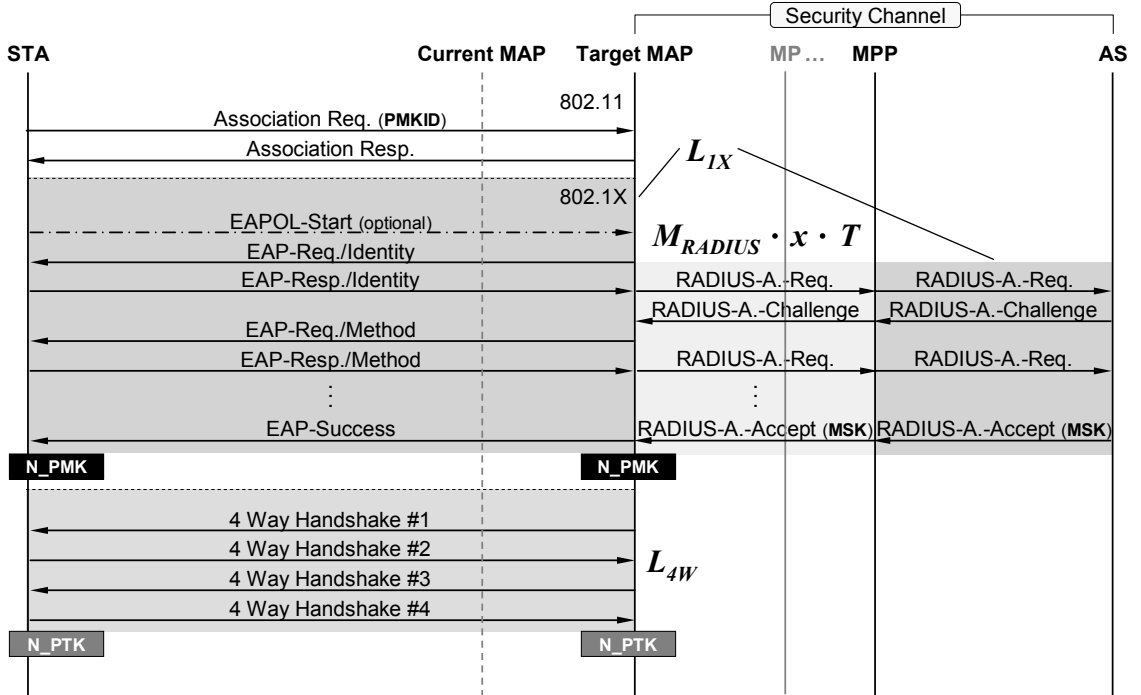


Figure 5-8 Intra-MPP handoff latency with 802.11i

For 802.11i, the intra-MPP handoff latency is shown as Figure 5-8. If the PMK is not cached by the target MAP, 802.1X authentication will be performed in the handoff.

$L_{INTRA\_AUTH}$  represents the average latency, where

$$L_{INTRA\_AUTH} = L_{IX} + M_{RADIUS} \cdot T \cdot H, \quad \text{802.11i} \quad (12)$$

- $L_{IX}$  is the latency for an STA performing 802.1X authentication in the single-hop network, i.e., WLAN.
- $M_{RADIUS}$  is the number of RADIUS messages exchanged between the target MAP and the AS in an 802.1X authentication.



In the handshake phase, the latency is the same in WLAN Mesh and WLAN.  $L_{INTRA\_4W}$  represents the latency, where

$$L_{INTRA\_4W} = L_{4W}, \quad 802.11i \quad (13)$$

- $L_{4W}$  is the latency for an STA performing 4-way handshake in WLAN.

Based on equations (8), (11), (12) and (13),  $L_{INTRA}$  is defined as

$$L_{INTRA} = (1 - P_{PMK\_MISS}) \cdot L_{INTRA\_4W} + P_{PMK\_MISS} \cdot (L_{INTRA\_AUTH} + L_{INTRA\_4W}) \quad (14)$$

$$P_{PMK\_MISS} = (1 - P_{REVISIT}) \cdot P_{PF} \quad (15)$$

- $P_{PMK\_MISS}$  is the probability that the PMK is not cached by the target MAP.
- $P_{REVISIT}$  is the probability that an STA moves to a visited cell or cluster.
- $P_{PF}$  is the probability that 802.11i preauthentication is failed.

Since the PMK is always cached by the authenticator, the intra-MPP handoff with ISD will only introduce  $L_{INTRA\_4W}$ . However, if an STA handoffs to a new MAP and fails to preauthenticate with it,  $L_{INTRA\_AUTH}$  will be introduced to the intra-MPP handoff with 802.11i.

### 5.2.1.2 Inter-MPP Handoff Latency

$L_{INTER}$  represents the latency for an STA performing the inter-MPP handoff, which consists of authentication latency ( $L_{INTER\_AUTH}$ ) and 4-way handshake latency ( $L_{INTER\_4W}$ ).

The inter-MPP handoff with ISD is shown as Figure 5-9. While the STA moves out of the cluster, if the PMK is not cached by the new MPP, 802.1X authentication will be performed.  $L_{INTER\_AUTH}$  represents the latency, where

$$L_{INTER\_AUTH} = L_{IX} + M_{IX} \cdot (n - 1) \cdot T, \quad ISD \quad (16)$$

- $M_{IX}$  is the number of EAPOL messages exchanged between the target MAP and the MPP in an 802.1X authentication.
- $n-1$  is the hop count between the target MAP and the new MPP.

An STA performing the inter-MPP handoff will reassociate with another boundary MAP in another cluster. Thus, the hop count between the target MAP and the new MPP is definitely  $n-1$ .

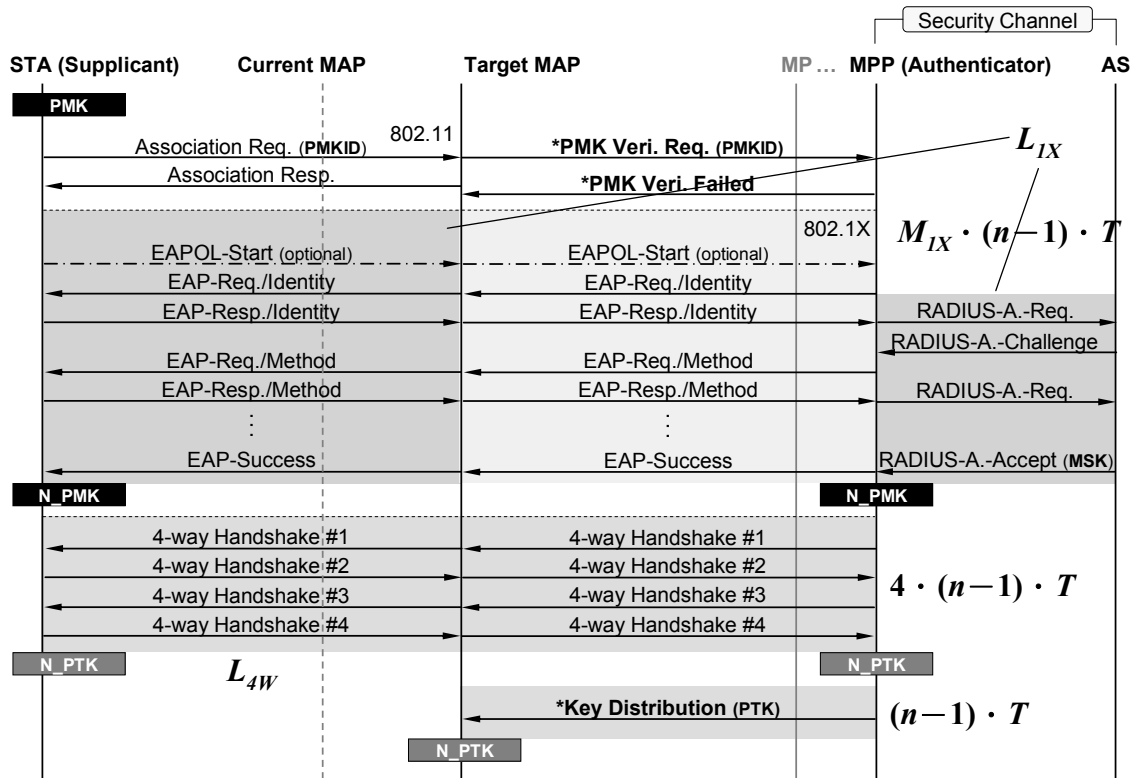


Figure 5-9 Inter-MPP handoff latency with ISD

$L_{INTER\_4W}$  represents the average latency for 4-way handshake and PTK distribution in the inter-MPP handoff, where

$$L_{INTER\_4W} = L_{4W} + 5 \cdot (n-1) \cdot T, \quad \text{ISD} \quad (17)$$

The inter-MPP handoff latency with 802.11i is shown as Figure 5-10, which is the same as the intra-MPP handoff, except messages are forwarded via the boundary MAP.

$L_{INTER\_AUTH}$  represents the authentication latency, where

$$L_{INTER\_AUTH} = L_{IX} + M_{RADIUS} \cdot (n-1) \cdot T, \quad 802.11i \quad (18)$$

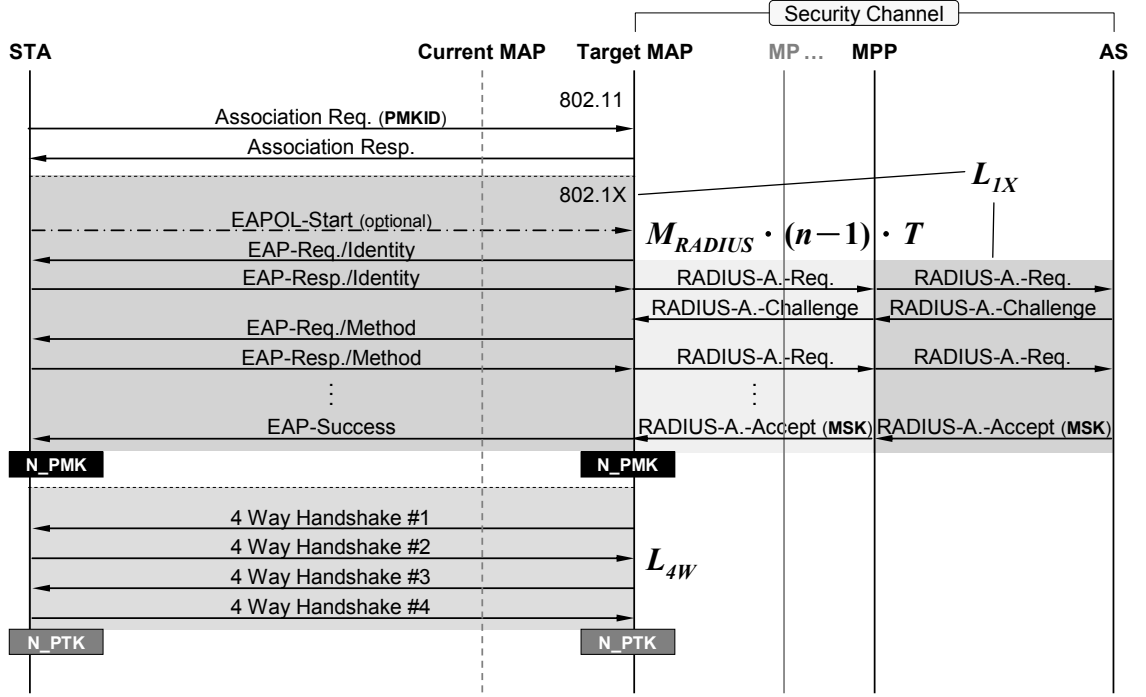


Figure 5-10 Inter-MPP handoff latency with 802.11i

$L_{INTER\_4W}$  represents the 4-way handshake latency, where

$$L_{INTER\_4W} = L_{4W}, \quad 802.11i \quad (19)$$

Based on equations (15), (16), (17) and (18),  $L_{INTER}$  is defined as

$$L_{INTER} = (1 - P_{PMK\_MISS}) \cdot L_{INTER\_4W} + P_{PMK\_MISS} \cdot (L_{INTER\_AUTH} + L_{INTER\_4W}) \quad (20)$$

For ISD, only an STA moves to an unvisited ISD and fails to perform preauthentication, the authentication latency is introduced to the inter-MPP handoff. However, for 802.11i, the STA will perform 802.1X authentication in each handoff in the same condition. Therefore, ISD can greatly reduce the demand for performing 802.1X authentication and provide the equivalent security strength as 802.11i.

## 5.2.2 Handoff Traffic

Even though the handoff traffic is much lower than the data traffic, to guarantee the QoS the authentication message should avoid contending with the real-time application message for the medium access.

The proposed equations can estimate the traffic in the mesh network generated by the security mechanism for an STA roaming within the WLAN Mesh. The preauthentication traffic is ignored, and the traffic is measured by the number of the normalized messages multiplied by the hop count. The handoff traffic can be classified into two types: intra-MPP handoff traffic ( $T_{INTRA}$ ) and latency inter-MPP handoff traffic ( $T_{INTER}$ ).

### 5.2.2.1 Intra-MPP Handoff Traffic

$T_{INTRA}$  represents the traffic generated by the security mechanism for an STA performing the intra-MPP handoff, which consists of authentication traffic ( $T_{INTRA\_AUTH}$ ) and 4-way handshake traffic ( $T_{INTRA\_4W}$ ).

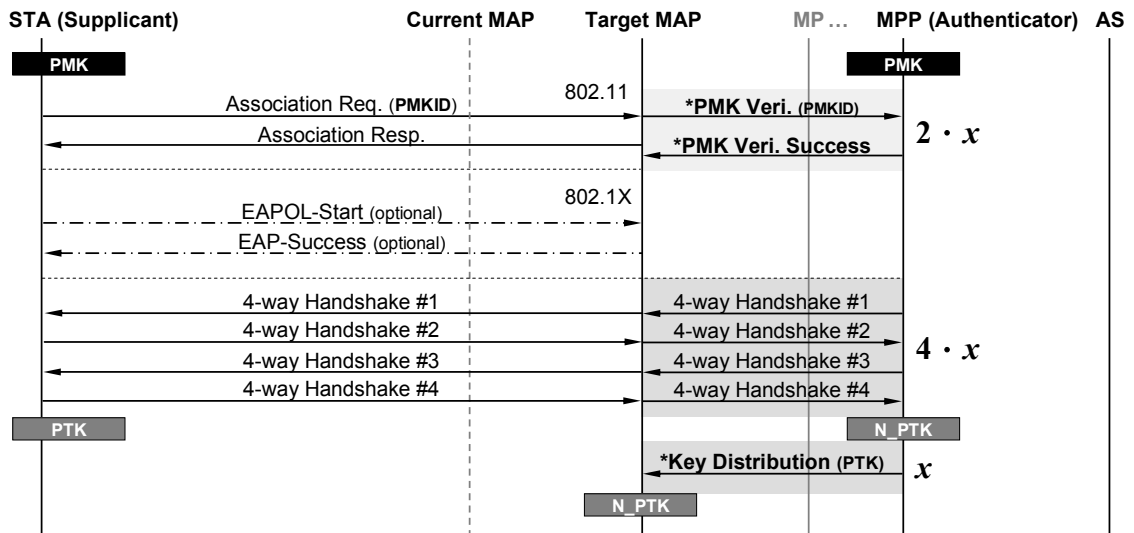


Figure 5-11 Intra-MPP handoff traffic with ISD

For ISD, as shown in Figure 5-11, there are 7 messages transmitted via the WLAN Mesh: 2 messages for the PMK verification, 4 messages for the 4-way handshake and 1 message for the PTK distribution.  $T_{INTRA\_AUTH}$  and  $T_{INTRA\_4W}$  represent the traffic, where

$$T_{INTRA\_AUTH} = 2 \cdot H, \quad \text{ISD} \quad (21)$$

$$T_{INTRA\_4W} = 5 \cdot H \cdot R, \quad \text{ISD} \quad (22)$$

- $R$  is ratio of 802.1X authentication to 4-way handshake in average message size.

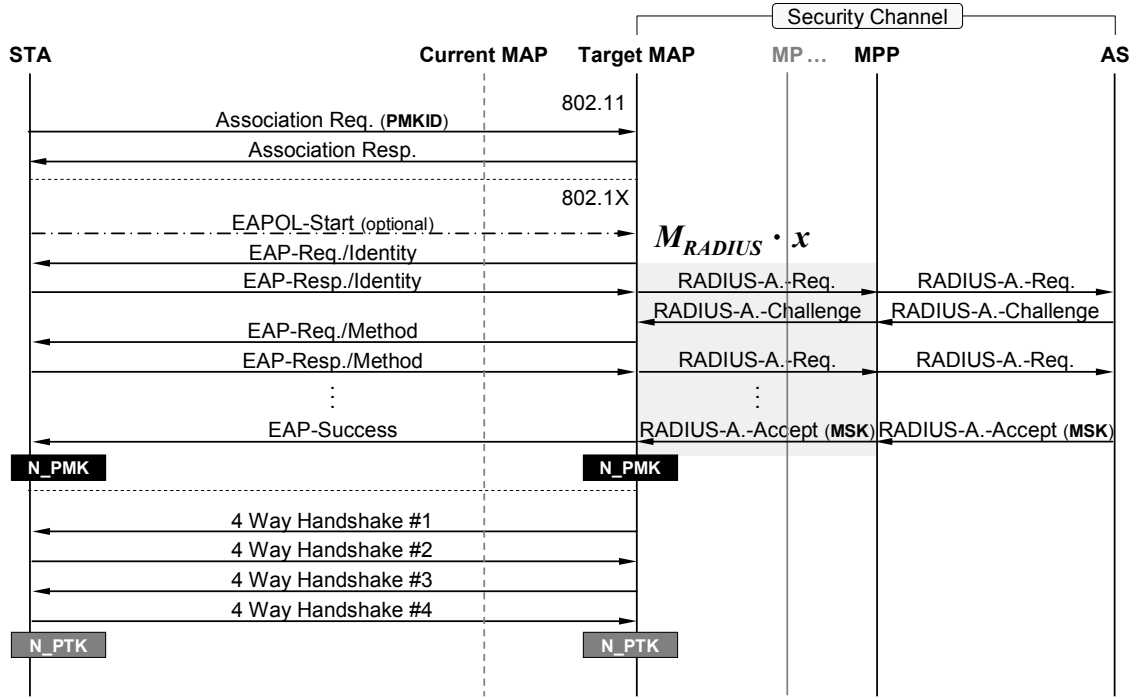


Figure 5-12 Intra-MPP handoff traffic with 802.11i

For 802.11i, as shown in Figure 5-12, only RADIUS messages are transmitted via the WLAN Mesh.  $T_{INTRA\_AUTH}$  and  $T_{INTRA\_4W}$  represent the traffic, where

$$T_{INTRA\_AUTH} = M_{RADIUS} \cdot H, \quad \text{802.11i} \quad (23)$$

$$T_{INTRA\_4W} = 0, \quad \text{802.11i} \quad (24)$$

Based on equations (21), (22), (23) and (24),  $T_{INTRA}$  is defined as

$$T_{INTRA} = (1 - P_{PMK\_MISS}) \cdot T_{INTRA\_4W} + P_{PMK\_MISS} \cdot (T_{INTRA\_AUTH} + T_{INTRA\_4W}) \quad (25)$$

### 5.2.2.2 Inter-MPP Handoff Traffic

$T_{INTER}$  represents the traffic generated by the security mechanism for an STA performing the inter-MPP handoff, which consists of authentication traffic ( $T_{INTER\_AUTH}$ ) and 4-way handshake traffic ( $T_{INTER\_4W}$ ).

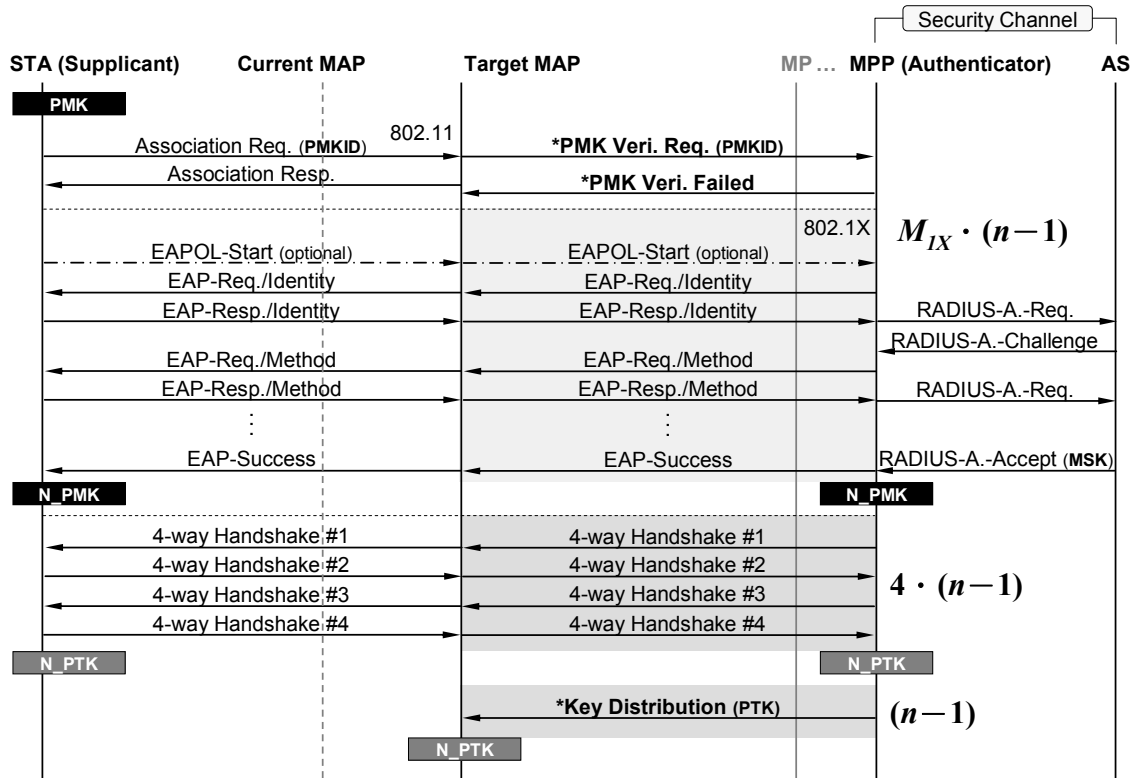


Figure 5-13 Inter-MPP handoff traffic with ISD

For ISD, as shown in Figure 5-13, all EAPOL messages and 4-way handshake messages are transmitted via the WLAN Mesh.  $T_{INTER\_AUTH}$  and  $T_{INTER\_4W}$  represent the traffic, where

$$T_{INTER\_AUTH} = M_{IX} \cdot (n-1), \quad \text{ISD} \quad (26)$$

$$T_{INTER\_4W} = 5 \cdot (n-1) \cdot R, \quad \text{ISD} \quad (27)$$

For 802.11i, as shown in Figure 5-14, the traffic is the same as the intra-MPP handoff traffic.  $T_{INTER\_AUTH}$  and  $T_{INTER\_4W}$  represent the traffic, where

$$T_{INTER\_AUTH} = M_{RADIUS} \cdot (n-1), \quad 802.11i \quad (28)$$

$$T_{INTER\_4W} = 0, \quad 802.11i \quad (29)$$

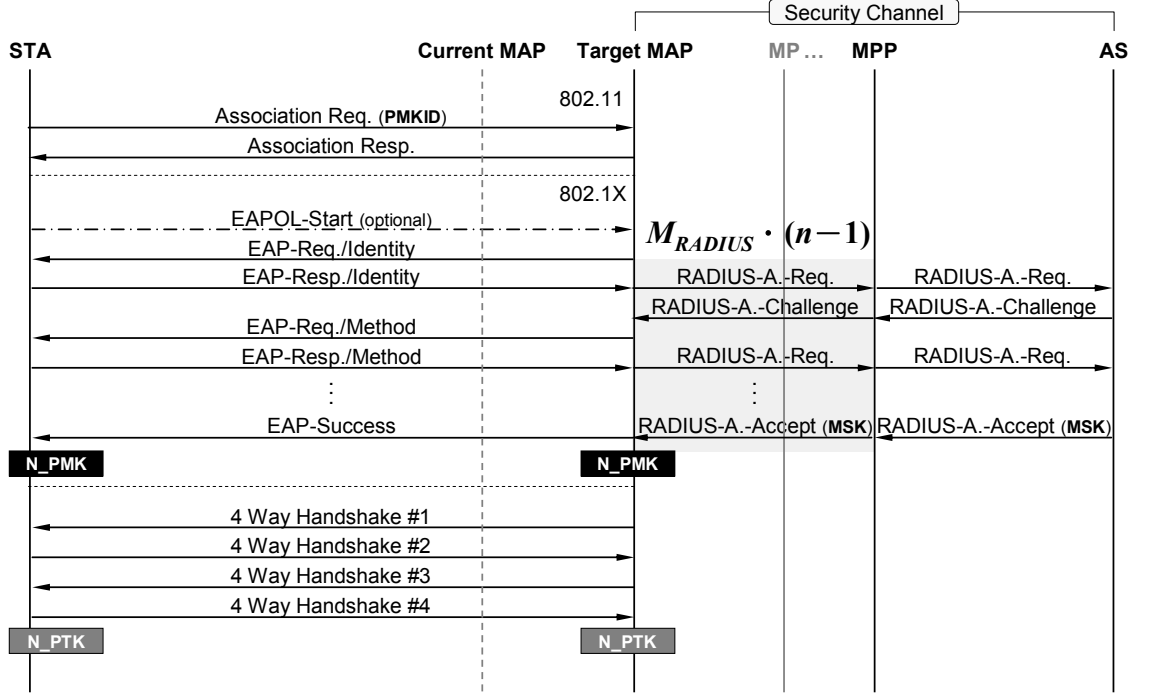


Figure 5-14 Inter-MPP handoff traffic with 802.11i

Based on equations (26), (27), (28) and (29),  $T_{INTER}$  is defined as

$$T_{INTER} = (1 - P_{PMK\_MISS}) \cdot T_{INTER\_4W} + P_{PMK\_MISS} \cdot (T_{INTER\_AUTH} + T_{INTER\_4W}) \quad (30)$$

### 5.2.3 Expected Handoff Overhead

Based on equations (8) (14), and (20), for an STA roaming within the WLAN Mesh, the expected handoff latency contributed by the security mechanism is defined as

$$L_S = \frac{\sum_{x=0}^{n-1} \sum_{y=0}^{x-1} \sum_{k=1}^{\infty} \sum_{j=0}^{n-2} P_{k,(x,y),(n,j)} \cdot \left[ \frac{(k-1)}{k} \cdot L_{INTRA} + \frac{1}{k} L_{INTER} \right]}{[1 + n(n-1)/2]} \quad (31)$$

Based on equations (8) (25), and (30), the expected handoff traffic is defined as

$$T_S = \frac{\sum_{x=0}^{n-1} \sum_{y=0}^{x-1} \sum_{k=1}^{\infty} \sum_{j=0}^{n-2} P_{k,(x,y),(n,j)} \cdot \left[ \frac{(k-1)}{k} \cdot T_{INTRA} + \frac{1}{k} T_{INTER} \right]}{[1 + n(n-1)/2]} \quad (32)$$

### 5.3 Experiment and Simulation

In order to obtain parameters of the equations, an experimental platform is built to measure the handoff latency, transmission time, the number of messages, etc. The experimental environment is shown in Figure 5-15, where the AS, two authenticators and the supplicant reside in a LAN.

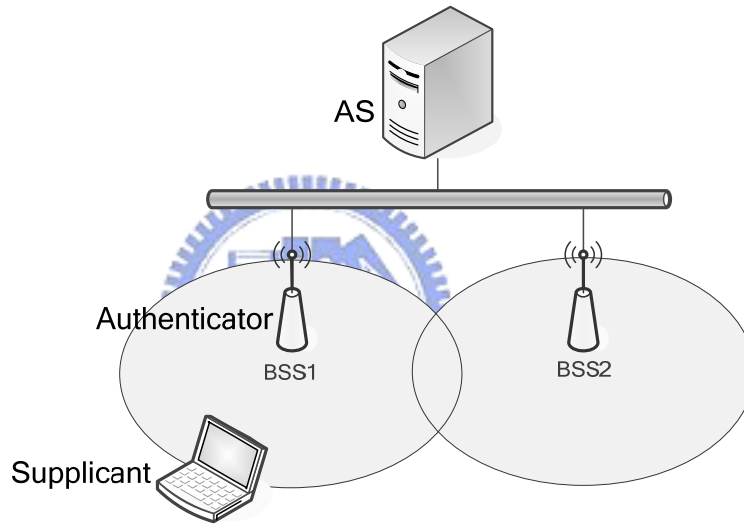


Figure 5-15 Experimental environment

The supplicant is a laptop installed Windows XP SP2, and the supplicant software is the build-in Windows Zero Configuration Service. Two authenticators are laptops controlled by the hostapd-0.5.7. The FreeRADIUS-1.1.4 is installed in the AS to provide the authentication services. The encryption mechanism is WPA2/AES<sup>6</sup>, and the EAP method is PEAP/EAP-MSCHAPv2.

Parameters are measured in the experimental platform. Table 5-1 presents the average measurement with 20 experiments.

<sup>6</sup> The patch KB893357 is necessary for Windows XP to provide support for WPA2.



Table 5-1 Parameters measured in the experimental platform

$T$	2.44 ms
$L_{IX}$	401.63 ms
$L_{4W}$	20.76 ms
$M_{IX}$	22 messages
$M_{RADIUS}$	18 messages
$R$	1.049180328

$P_{REVISIT}$  is calculated with 1,200,000 simulations. Table 5-2 presents results from 1-subarea cluster to 8-subarea cluster.

Table 5-2 Average  $P_{REVISIT}$  calculated in the simulation

$n = 1$	0.000000
$n = 2$	0.064579
$n = 3$	0.120625
$n = 4$	0.164704
$n = 5$	0.199851
$n = 6$	0.229387
$n = 7$	0.254347
$n = 8$	0.275391

## 5.4 Results

Figure 5-16 presents the relationship between  $P_{PF}$  and  $L_S$  at  $n = 3$ . Estimated results show that ISD remarkably reduces the handoff latency. At  $P_{PF} = 1.0$ , i.e., STA does not perform preauthentication, ISD can improve the handoff latency up to 245%. Therefore, even though most of current 802.11i devices do not support preauthentication<sup>7</sup>, STAs can still take advantage of ISD. However, at  $P_{PF} < 0.05$ , due to 4-way handshake mes-

<sup>7</sup> The preauthentication function in Windows XP with WPA2 is disabled in default.

sages are forwarded between MAP and MPP, ISD introduces larger  $L_S$ , than 802.11i.

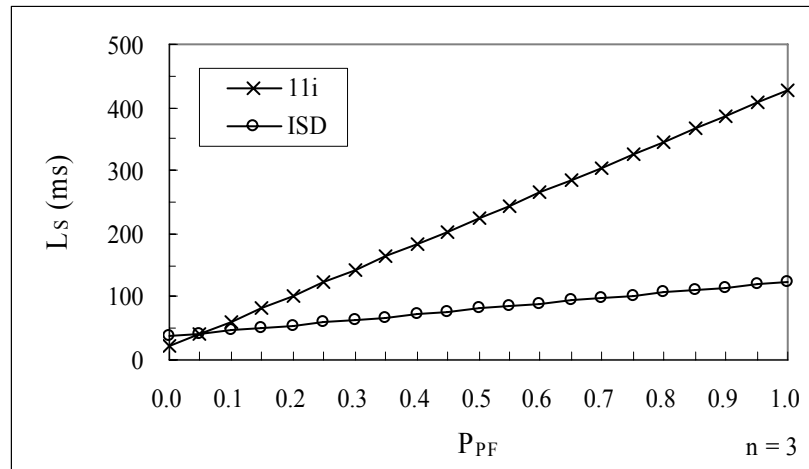


Figure 5-16 Handoff latency with different  $P_{PF}$

Figure 5-17 presents  $L_S$  with different cluster sizes at  $P_{PF} = 1.0$ . At  $n = 5$ , ISD approaches the minimal  $L_S$ . Actually, the handoff latency of ISD is almost stable at  $n > 3$ .

For ISD, the burden incurred by the multi-hop transmission in the 4-way handshake counteracts the benefit of the larger cluster size. For 802.11i, EAP authentication is also delayed by the multi-hop transmission, and thus  $L_S$  increases with the growing cluster size.

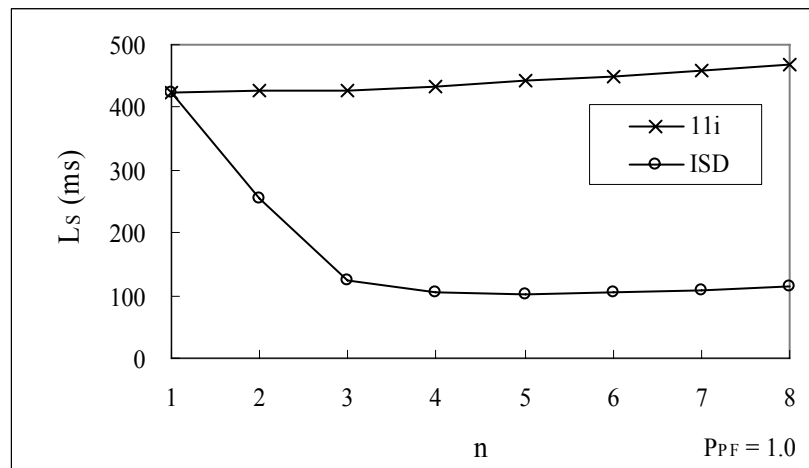


Figure 5-17 Handoff latency with different  $n$

$L_S$  of ISD with different cluster sizes and  $P_{PF}$  are shown in Figure 5-18. Results indicate that the larger cluster size avail the handoff latency in all kinds of  $P_{PF}$ . Besides,

the influence of  $P_{PF}$  is decreasing with the growing cluster size.

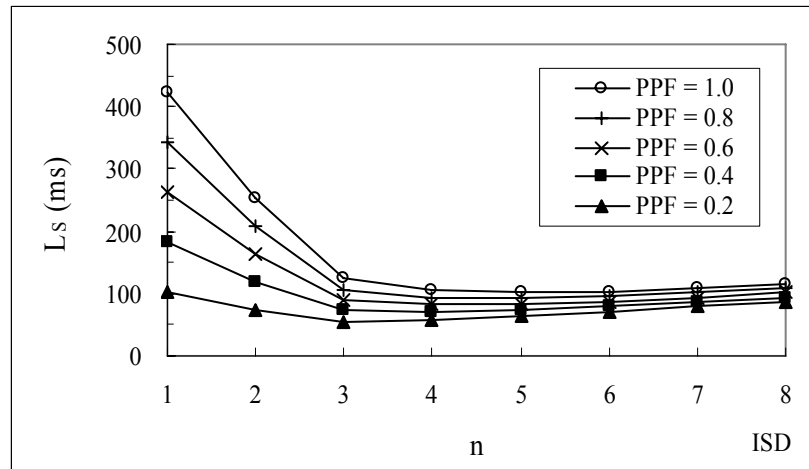


Figure 5-18 Handoff latency of ISD with different  $n$  and  $P_{PF}$

The improvement of ISD to the 802.11i with different  $L_{IX}$  is shown in Figure 5-19. Results show that the longer  $L_{IX}$  favors ISD. Therefore, no matter AS resides in the local or remote network, ISD can improve the handoff latency greatly.

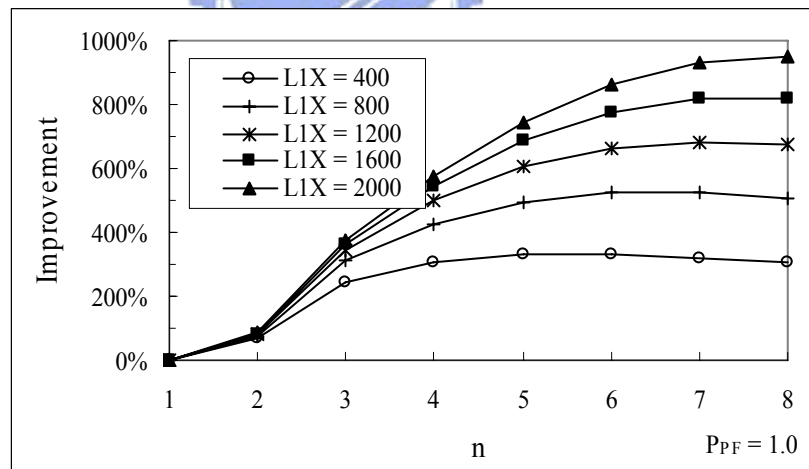


Figure 5-19 Improvement of ISD with different  $n$  and  $L_{IX}$

In the condition that ISD and 802.11i generate the equal handoff latency, Figure 5-20 represents the relationship between ISD with different cluster sizes at  $P_{PF} = 1.0$  and 802.11i with different  $P_{PF}$ . Results indicate that the handoff latency of ISD is equivalent to 802.11i performing preauthentication at  $P_{PF} = 0.2-0.1$ . It means ISD provides around 80%-90% successful probability for preauthentication without any addi-

tional assistance, such as network topology information or historical handoff behaviors.

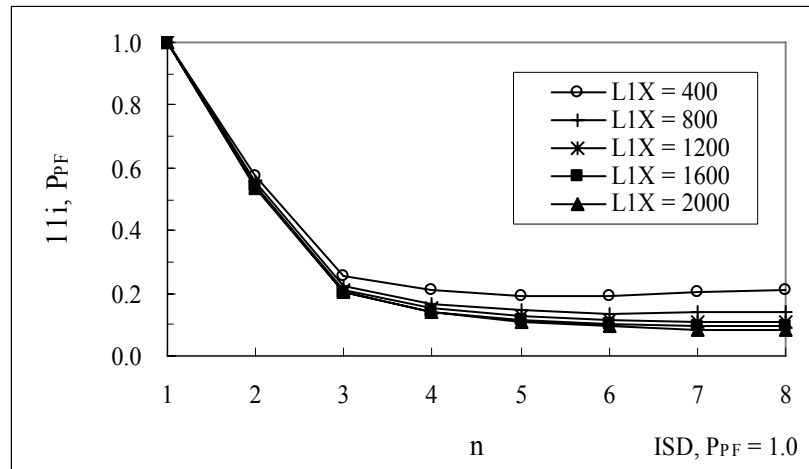


Figure 5-20 Relationship between ISD and 802.11i in the equal  $L_s$

The MP topology of WLAN Mesh may be different with the proposed handoff model. Figure 5-21 presents the handoff latency with different average hop counts between MAP and MPP. Results indicate that ISD can remarkably improve the handoff latency in all average hop counts, which means ISD can be applied to varied MP topologies.

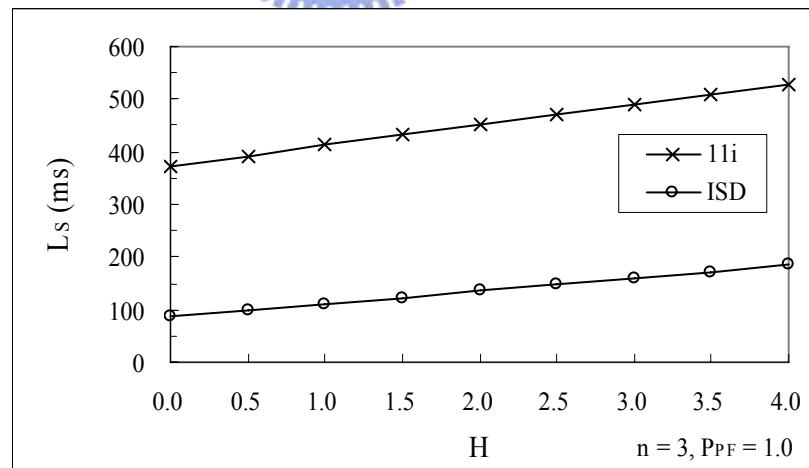


Figure 5-21 Handoff latency with different  $H$

ISD essentially reduces the demand of 802.1X authentication but incurs the burden of the multi-hop latency in 4-way handshake. Since 802.1X authentication latency is much longer than the message transmission time, the benefit of ISD is certainly much

larger than the burden in terms of the handoff latency.

Figure 5-22 presents the relationship between  $P_{PF}$  and  $T_S$  at  $n = 3$ . Due to ISD is a centralized architecture, 4-way handshake messages are forwarded to MPP via the WLAN Mesh. At  $P_{PF} < 0.55$ , ISD generates more handoff traffic than 802.11i. However, whereas  $P_{PF}$  is low, the handoff traffic will not burden the network.

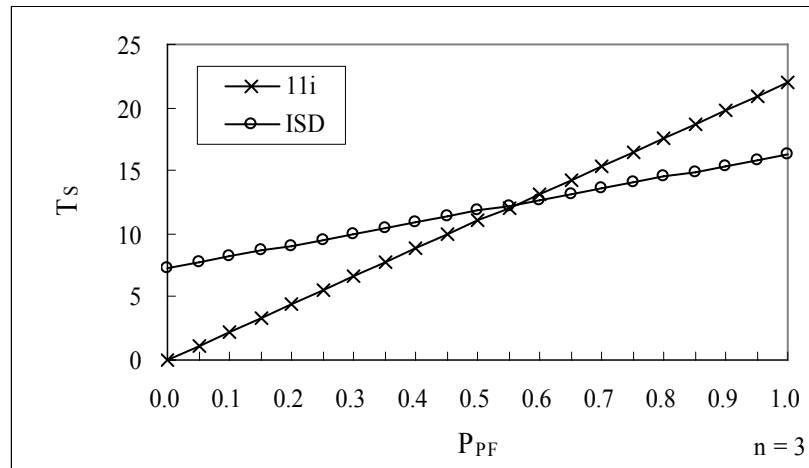


Figure 5-22 Handoff traffic with different  $P_{PF}$

Figure 5-23 presents  $T_S$  with different cluster sizes at  $P_{PF} = 1.0$ . Results indicate that the handoff traffic generated by ISD is less than 802.11i except at  $n = 2$ . It means the benefit of reducing the number of handoffs in the larger cluster size exceeds the overhead of the growing hop count.

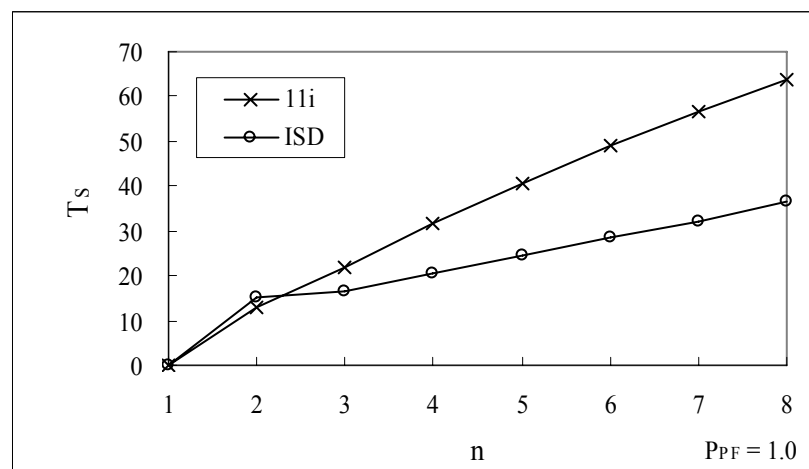


Figure 5-23 Handoff traffic with different  $n$

Figure 5-24 presents the handoff traffic with different average hop counts between MAP and MPP. Results indicate that ISD can reduce the handoff traffic in all average hop counts, which means ISD can be applied to varied MP topologies.

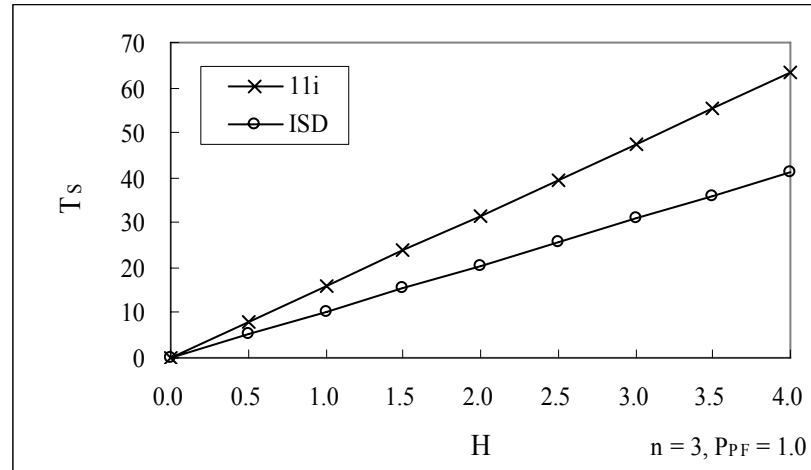


Figure 5-24 Handoff traffic with different  $H$

According to the estimated results, we can conclude that ISD provides great improvement in the handoff latency when the cluster size is around 3 layers, i.e., 37 MPs connect to one MPP. This number accords with the scale of the 802.11s standard.

ISD is practical to use in current wireless environments. In terms of the power consumption, ISD estimates 802.11X authentication, and thus the battery-powered STA can balance the power consumption and the handoff performance. Furthermore, since the AS mostly resides in the core network,  $L_{IX}$  would be longer than 400 ms. Estimated results indicate that ISD can further improve the handoff latency in this environment.

Even though ISD is the centralized architecture and forwards 4-way handshake messages to MPP, it does not result in the extra overhead in the handoff traffic. Actually, ISD can reduce the handoff traffic in all kinds of mesh networks at  $P_{PF} = 1.0$ .

## Chapter 6

### Conclusion and Future Work

The authentication latency is a key factor for supporting the seamless handoff. To improve the handoff latency, ISD is proposed to remove 802.1X authentication from the handoff.

Another problem is the routing performance of WLAN Mesh. The hop-by-hop encryption delays the routing processing of MPs. An end-to-end security channel is provided by ISD to solve this problem.

Another advantage of ISD is the compatibility to current 802.11i/11s devices. STAs can apply the proposed mechanism without any modification. Besides, ISD is an optional feature to WLAN Mesh. Original security and routing mechanism of the 802.11s standard can co-operate with ISD.

To evaluate the handoff latency introduced by the link layer security mechanism, we propose a handoff model to estimate the handoff latency for an STA roaming within the WLAN Mesh. Results indicate that ISD improves the handoff latency up to 245% and provides 80%-90% successful preauthentication probability without any assistance.

Our future works focus on three portions. First, to evaluate the routing performance, we need to implement ISD on the WLAN Mesh. The implementation can base on the open source software, hostapd. Second, proposed estimation equations can be used to evaluate other handoff mechanisms, such as 802.11r or 802.16e. The estimated results provide the quantitative analysis to the handoff latency, and the performance of the implementation can be evaluated. Finally, to achieve the goal of the seamless handoff, re-authentication mechanisms of conventional EAP methods have to be optimized. This

has been addressed by IETF, and a new working group called Handover Keying<sup>8</sup>, is composed for improving current unacceptable latency of EAP authentication in mobile wireless environments.



---

<sup>8</sup> <http://www.ietf.org/html.charters/hokey-charter.html>



## Bibliography

- [1] B. Aboba, et al., “Extensible Authentication Protocol (EAP),” IETF RFC 3748, June 2004.
- [2] B. Aboba, et al., “Extensible Authentication Protocol (EAP) Key Management Framework,” IETF Draft draft-ietf-eap-keying-17, January 2007.
- [3] I. F. Akyildiz, et al., “Wireless Mesh Networks: A Survey,” Computer Networks Journal, vol. 47, no. 4, pp. 445-487, March 2005.
- [4] I. F. Akyildiz, et al., “A New Random Walk Model for PCS Networks,” IEEE Journal on Selected Areas in Communications, vol. 18, no. 7, pp. 1254-1260, July 2000.
- [5] A. Alimian and B. Aboba, “Analysis of Roaming Techniques,” IEEE 802.11 Contribution 802.11-04/0377r1, March 2004.
- [6] M. S. Bargh, et al., “Fast Authentication Methods for Handovers between IEEE 802.11 Wireless LANs,” 2nd ACM Int. WMAS, pp. 51-60, Philadelphia, USA, October 2004.
- [7] P. Calhoun, et al., “CAPWAP Protocol Binding for IEEE 802.11,” IETF Draft draft-ietf-capwap-protocol-binding-ieee80211-03, April 2007.
- [8] Y. R. Chiang and C. C. Tseng, “Design and Implementation of a Topology-Aware Seamless Handover for IEEE 802.11 Wireless Networks,” National Chiao Tung University, Master Thesis, June 2006.
- [9] W. S. Conner, et al., “IEEE 802.11s Tutorial: Overview of the Amendment for Wireless Local Area Mesh Networking,” IEEE 802 Plenary, Dallas, USA, November 2006.
- [10] M. S. Gast, 802.11 Wireless Networks: The Definitive Guide, Second Edition,

O'Reilly, USA, April 2005.

- [11] IEEE 802.1 Working Group, "Port-Based Network Access Control," IEEE Standard 802.1X-2004, December 2004.
- [12] IEEE 802.11 Working Group, "Amendment 6: Medium Access Control (MAC) Security Enhancements," IEEE Standard 802.11i-2004, July 2004.
- [13] IEEE 802.11 Working Group, "Amendment 2: Fast BSS Transition," IEEE Standard Draft P802.11r/D4.0, November 2006.
- [14] IEEE 802.11 Working Group, "Amendment: ESS Mesh Networking," IEEE Standard Draft P802.11s/D1.0, November 2006.
- [15] R. H. Jan and Y. C. Huang, "Fast Pre-authentication based on IEEE 802.11i," 2nd WASN, pp. 317-324, Taoyuan, Taiwan, August 2006.
- [16] A. Mishra, et al., "Pro-active Key Distribution using Neighbor Graphs," IEEE Wireless Communication Magazine, vol. 11, no. 1, pp. 26-36, February 2004.
- [17] A. Mishra, et al., "An Empirical Analysis of the IEEE 802.11 Mac Layer Handoff Process," ACM SIGCOMM Computer Communication Review, vol. 33, pp. 93-102, April 2003.
- [18] S. Pack and Y. Choi, "Fast Inter-AP Handoff Using Predictive Authentication Scheme in a Public Wireless LAN," Networks 2002, pp.15-26, Atlanta, USA, August 2002.
- [19] S. Pack and Y. Choi, "Pre-Authenticated Fast Handoff in a Public Wireless LAN Based on IEEE 802.1X Model," IFIP Personal Wireless Communications 2002, pp. 175-182, Singapore, October 2002.
- [20] M. G. Rahman and H. Imai, "Security in Wireless Communication," Wireless Personal Communications, vol. 22, pp. 213-228, August 2002.
- [21] G. Xue, "An Improved Random Walk Model for PCS Networks," IEEE Transactions on Communications, vol. 50, no. 8, pp. 1224-1226, August 2002.