國立交通大學

資訊科學與工程研究所

碩士論文

以憑證為基礎的無線網路快速認證機制

Certificate Authority-Based Fast Authentication Mechanism for Wireless Networks

研究生：胡佳君

指導教授：曾建超　教授

葉義雄　教授

中華民國九十七年六月

以憑證為基礎的無線網路快速認證機制

Certificate Authority-Based Fast Authentication Mechanism for Wireless Networks

研究生：胡佳君　　Student：Chia-Chun Hu

指導教授：曾建超　　Advisor：Chien-Chao Tseng

葉義雄　　Yi-Shiung Yeh

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
June 2008
Hsinchu, Taiwan, Republic of China

中華民國九十七年六月

以憑證為基礎的無線網路快速認證機制

學生： 胡佳君　　　　　　　　　　指導教授：曾建超 博士

葉義雄 博士

國立交通大學資訊科學與工程研究所碩士班

摘要

無線通訊已成為日常生活的一部分，使用者可邊移動邊使用網路。隨著技術發展與成熟，整合不同的無線通訊系統，可跨不同ISP、網路種類，以提供使用者更方便的通訊服務。而漫遊時的重新認證很耗時間，會造成網路斷線，所以快速認證是達到無間隙漫遊所必需的。

為了達到無間隙漫遊的目標，系統必須提供下列功能： 1.在跨網域的漫遊能快速認證。 2.使用者目前漫遊到的網路可不需要與使用者的Home domain有漫遊協定，卻可以允許通過認證。 3.目前漫遊到的網路可對使用者作完整的認證，以確認使用者為合法的。然而目前的快速認證方法都無法完整滿足這些需求。

為了達到上述需求，本論文根據下列策略提出一跨無線通訊網域之快速認證方法： 1. 基於Extension of IAPP，讓AP間可以溝通，傳送必須的認證資訊，以達到快速認證。 2. 使用Certificate chain讓使用者與目前漫遊到的網路可以做完整的認證，卻不需要回到後端RADIUS伺服器。

Certificate Authority-Based Fast Authentication Mechanism for Wireless Networks

Student : Chia-Chun Hu **Advisor：Chien-Chao Tseng**

Yi-Shiung Yeh

Institute of Computer Science and Engineering

National Chiao Tung University

Abstract

Wireless network communications have already been a part of life, and users can connect to the network on the move. With the development and maturity of mobile communication technologies, a mobile subscriber can now roam across various communication systems with different network providers. However, the long authentication delay during handover may result in communication interruptions or even connection losses. Therefore, it is necessary to reduce the authentication delay for handover across networks or network provider domains.

For achieving the target of seamless handover across networks and domains, the handover mechanism should have the following characteristics: (1) fast authentication in inter-domain handovers, (2) no *a priori* roaming agreement directly between the domain a user is entering and the user’s home domain, and (3) re-authentication of a user in the visited domains. However, none of the existing fast authentication methods can fulfill these requirements.

In order to achieve the above-mentioned requirements, this thesis proposes a Certificate Authority-Based Fast Authentication Mechanism for Wireless Networks. The fast authentication mechanism adopts the following two underlying concepts: Extended Inter-Access Point Protocol (IAPP) and Certificate Chains. Extended IAPP enables authentication information exchanges between two access points and

Certificate Chains make it possible to perform re-authentication locally between a user and the visited AP without invoking remote authentication servers. With the Certificate Authority-Based Authentication Mechanism, we can reduce the authentication delay during handover to achieve fast handovers.

致謝

這篇論文能夠順利完成，首先要感謝我的指導教授，葉義雄教授與曾建超教授，教導我許多學問上的寶貴知識，並且在生活態度方面也讓我受益良多；兩位教授的學術專業與待人處世，均為我的表率。

接著特別要感謝銘智學長與靜紋學姊，在論文研究和兩年學習過程中不厭其煩地給予我許多指導與意見。還有要感謝實驗室的各位學長姊及同學們，定宇學長、鎮宇學長、韓禹學長、嘉耀學長、龍哥、欣諭學長、雅婷、文浩、Gobby、伯昕、小強與家明，謝謝你們的陪伴。此外，還要謝謝 Jerry 幫我修改英文及支持。

最後，要感謝我的父母多年來辛苦的栽培與支持，因為有你們，才能有今天的我。

僅將這篇論文獻給所有關心我與支持我的人，謝謝你們。

胡佳君

中華民國九十七年六月

Contents

List of Figures

List of Table

Chapter 1 Introduction

1.1 Background and motivation

With the development and maturity of mobile communication technology, users can easily link to network on the move. The enhancement of hardware technology results in compact and powerful mobile terminals that are easy to carry about. Wireless networks which transmit data by radio waves can satisfy the requirement of accessing network mobility. Nowadays, people heavily rely on mobile services in daily life. However, radio frequency is a public resource. Without a well-designed mechanism for network accessing, data transmitted via radio waves is easy to be obtained and misused.

802.11 is an IEEE standard for wireless local area network (WLAN). According to IEEE 802.11, users can access network resources of WLAN by mobile nodes (MN). Every WLAN contains several Access Points (AP) to provide radio access service. But the coverage of an AP is bounded, and MS needs to change connection to other APs if it is out the coverage of the original AP during ongoing. The process that MN changes the connected AP is called handover. Handover within the same Extended Service Set (ESS) is called intra-domain handover, and handover across different domains is called inter-domain handover. Long handover delay will result in lose of connection, therefore, handover delay should be short enough to comply with the QoS (quality of service) requirement of mobile communications.

Authentication is an important part of the handover procedures to ensure the validity of connection. However authentication process often needs complex mathematical computation that consumes many computation power and long operation time. Therefore reducing authentication delay will effectively shorten handover delay. Many researches proposed fast authentication methods to reduce authentication time without losing authentication requirement, including proactive key distribution, pre-authentication, fast handover method using extending IAPP and roaming key. However, these methods have strong restrictions such as needing mutual roaming agreements among domains that may not be practical in the physical communication environment. In this thesis, we study the requirements of network operators and mobile communication users, and based on the communication scenarios we propose a fast authentication method to fulfill mobile user and equipment authentication. The evaluation of feasibility and efficiency of this method is also reported in this thesis.

1.2 Organization

The rest of this thesis is organized as in the following: Chapter 2 introduces the relative knowledge includes WLAN authentication, digital certificate, and some proposed protocols for fast authentication in handover. In chapter 3, we propose a fast handover method and illustrate the detail procedures. In chapter 4, we analysis the characteristics of our method and compare the present methods with our method. Finally, chapter 5 is the conclusion.

Chapter 2 Related knowledge

2.1 WLAN authentication

The transmission media of wireless networks transmit by radio waves. Unlike wired networks, wireless networks can not guarantee physical protection and security by protecting transmission media and equipments. Wireless networks need additional encryption and authentication to protect the data and confirm validity. In this chapter we introduce the protocols and procedures of wireless network authentication.

2.1.1 802.1X

IEEE 802.1X is an IEEE standard for port-based network access control. Taking into accounting of communication security, IEEE 802.1X involves a method and policy to authenticate users. Before authentication succeeds, access pointer (AP) filters messages without being following the authentication mechanism (non-EAPOW messages) from client. If authentication succeeds, AP lets client pass the port to establish network connection. [2]

There are some advantages of 802.1X that make it is been used popularly in network communication. The first advantage of 802.1X is extensible authentication support. Authentication in 802.1X is done in server and client application. AP and client NIC (Network Interface Card) are only the media which pass the messages securely between server and client. Therefore, it does not require additional changes to AP and client NIC while authentication methods are being modified. The other advantages of 802.1X are supporting dynamic key management, centralizing user administration in RADIUS, based on open standards like EAP and RADIUS, and user-based identification [2].

Following is the description of the components of IEEE 802.1X authentication mechanism: [1]

(1) Supplicant

A supplicant is usually a terminal user device that supports 802.1X authentication, and is authenticated by an authenticator.

(2) Authenticator

An authenticator is usually a network device that supports 802.1X authentication which receives authentication requests from a supplicant and provides port for the supplicant.

(3) Authentication Server

An authentication server (AS) provides authentication service to an authenticator. This service verifies the credential of the supplicant, and responses the claims made by the supplicant.

Usually the AS is a RADIUS [3][4] server. RADIUS is Remote Authentication Dial In User Service which provides AAA(Authentication、Authorization、Accounting) service. Authentication service verifies the identity and password of a user. If authentication succeeds, authorization service authorizes user to use available network resource and accounting service records the information of user.

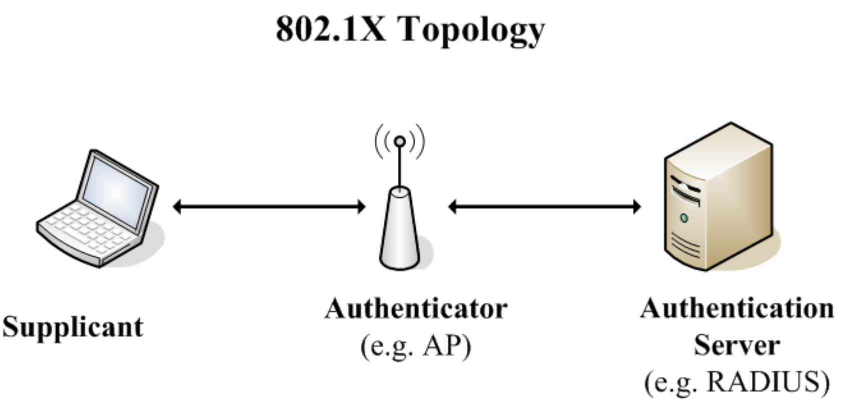


Figure 2.1 802.1X topology

2.1.2 EAP

EAP [10] is the abbreviation of "Extensible Authentication Protocol". It is an authentication framework which supports multiple authentication methods. There are currently about 40 different methods defined in IEFT RFCs including EAP-MD5, EAP-TLS, EAP-TTLS, EAP-LEAP, EAP-PEAP, EAP-SIM, and EAP-AKA and so on. EAP runs directly over data link layers such as Point-to-Point Protocol (PPP) [5], without requiring IP.

Figure 2.2 illustrates the IEEE 802.1X conversation on 802.11. After 802.11 associates, AP blocks the non-EAPOW packets from client. EAPOW means EAP over WLAN. The first EAPOW packet is EAPOW-Start sent by client. Then AP requests the identity and password of client. After client response the identity and password to AP, AP transmits those to RADIUS server. RADIUS server authenticates client through AP. If authentication succeeds, RADIUS server informs AP to let packets of client to pass the port and access network.

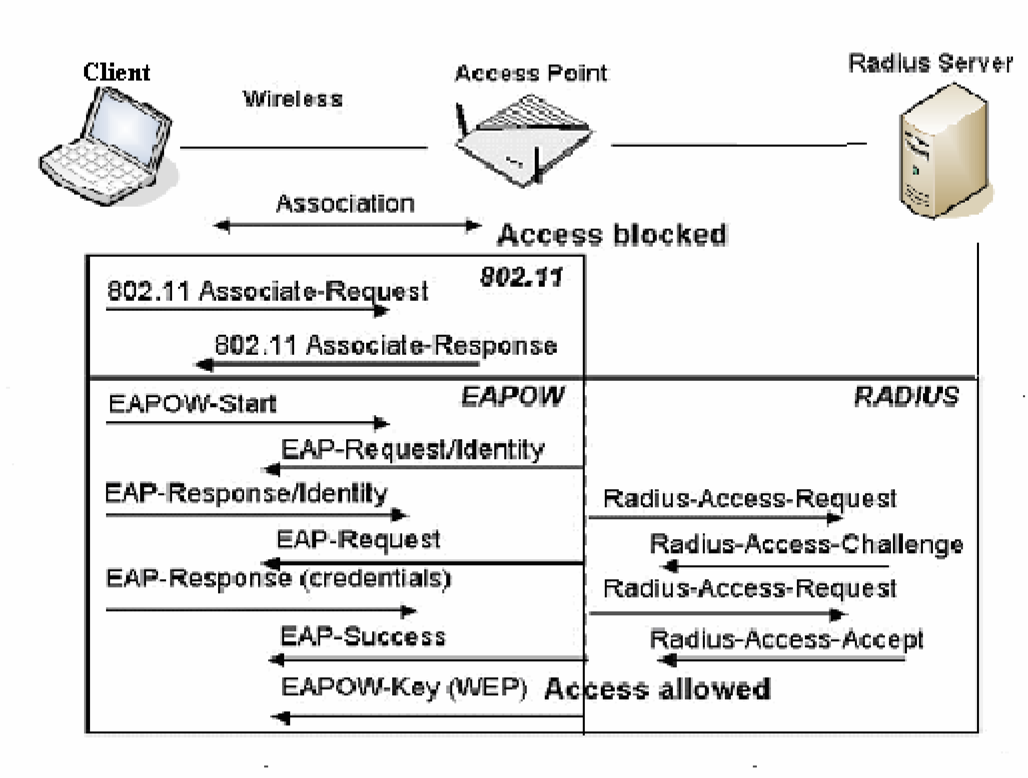


Figure 2.2 EAP over 802.1X

RADIUS server has a list to record the valid APs which belong to it. After authentication, client and RADIUS server can trust each other by explicit trust via EAP authentication. The trust relation between client and AP is implicit trust. Client connects to RADIUS via the AP therefore it knows that the AP is trusted by RADIUS. Besides that, client and AP also can trust each other by secret keys distribution which is discussed in chapter 2.1.4.

2.1.3 EAP-TLS

EAP-TLS or EAP-Transport Level Security is an authentication method defined in RFC 5216. It uses PKI (Public Key Infrastructure) for security communication. Client and server can mutually authenticate using certificates (Chapter 2.2). Server sends its certificate to client. Then client uses the public key of issuer (CA) to verify the certificate of server. Client sends its certificate to server. Then server uses the public key of issuer (CA) to verify the certificate of client.

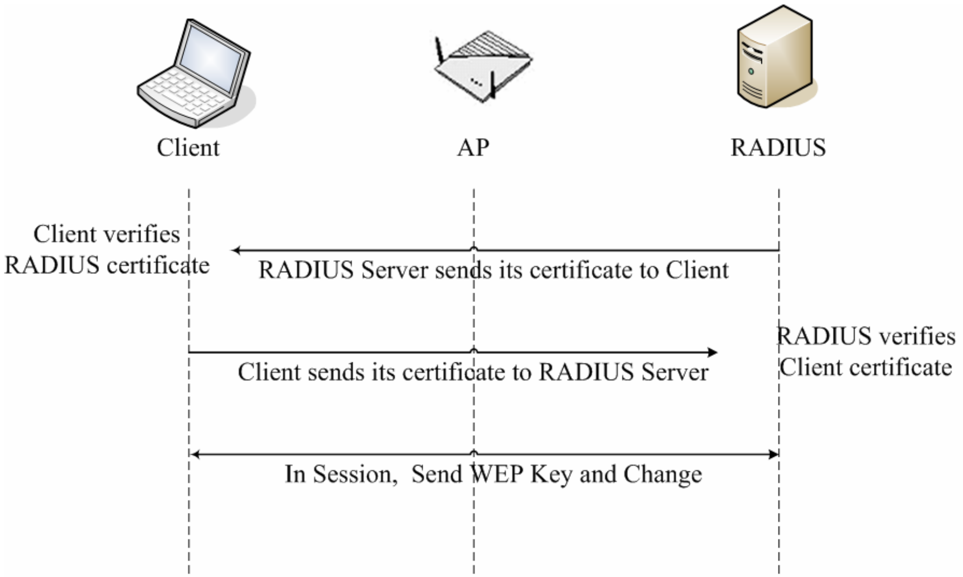
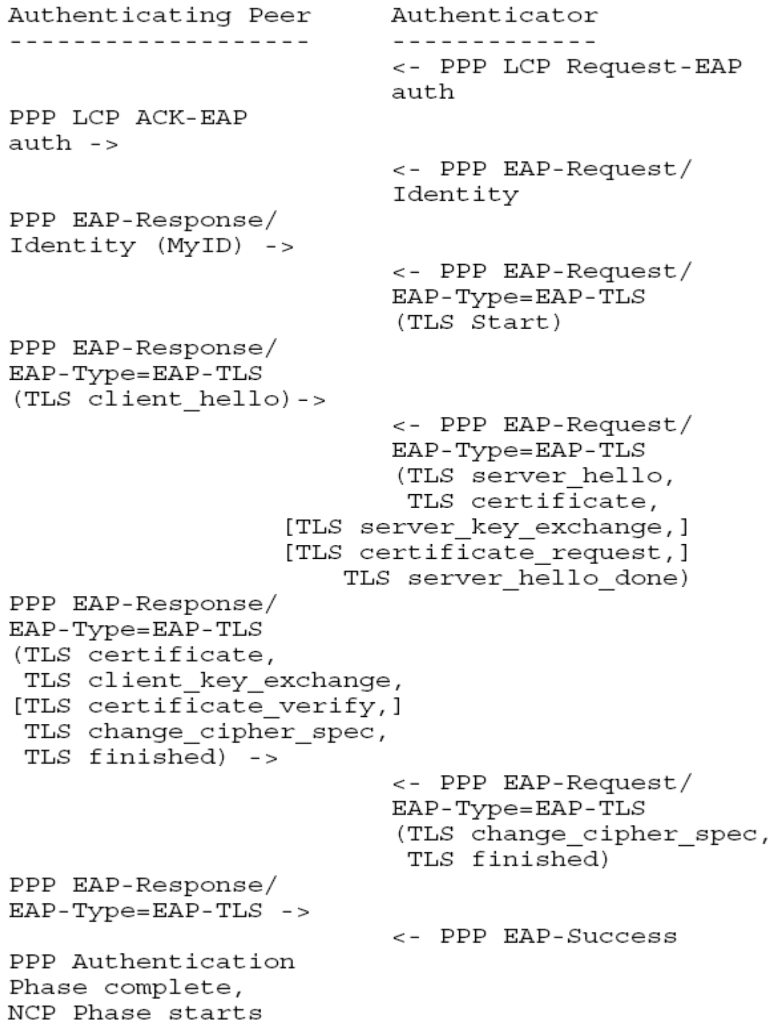

Client
AP
RADIUS
Client verifies RADIUS certificate
RADIUS Server sends its certificate to Client
RADIUS verifies Client certificate
Client sends its certificate to RADIUS Server
In Session, Send WEP Key and Change

Figure 2.3 EAP-TLS

Below is the description of the EAP-TLS full authentication processes from RFC5216 [6]:



```
Authenticating Peer     Authenticator
-------------------     -------------
                        <- PPP LCP Request-EAP
                        auth
PPP LCP ACK-EAP
auth ->
                        <- PPP EAP-Request/
                        Identity
PPP EAP-Response/
Identity (MyID) ->
                        <- PPP EAP-Request/
                        EAP-Type=EAP-TLS
                        (TLS Start)
PPP EAP-Response/
EAP-Type=EAP-TLS
(TLS client_hello)->
                        <- PPP EAP-Request/
                        EAP-Type=EAP-TLS
                        (TLS server_hello,
                         TLS certificate,
                 [TLS server_key_exchange,]
                 [TLS certificate_request,]
                     TLS server_hello_done)
PPP EAP-Response/
EAP-Type=EAP-TLS
(TLS certificate,
 TLS client_key_exchange,
[TLS certificate_verify,]
 TLS change_cipher_spec,
 TLS finished) ->
                        <- PPP EAP-Request/
                        EAP-Type=EAP-TLS
                        (TLS change_cipher_spec,
                         TLS finished)
PPP EAP-Response/
EAP-Type=EAP-TLS ->
                        <- PPP EAP-Success
PPP Authentication
Phase complete,
NCP Phase starts
```

Figure 2.4 Full authentication processes of EAP-TLS

2.1.4 Key management

IEEE 802.11i proposes a key management method which uses EAP/802.1X mechanisms. After 802.1X authentication, AS and client generate the same key, Mater Key (MK), by itself. Then AS and client generate the Pairwise Mater Key (PMK) from MK. AS sends the PMK to AP which client is associating with. Then client and AP do 4-way handshake to prove the liveness and legality of both peers by confirming the PMK. Therefore client and AP construct an implicit trust relation between each other. And client and AP derive the Pairwise Transient Key (PTK) via 4-way handshake for encrypting later data transmission. AP derives a Group Transient Key (GTK) and broadcasts GTK to all associated clients using 2-way handshake [8].

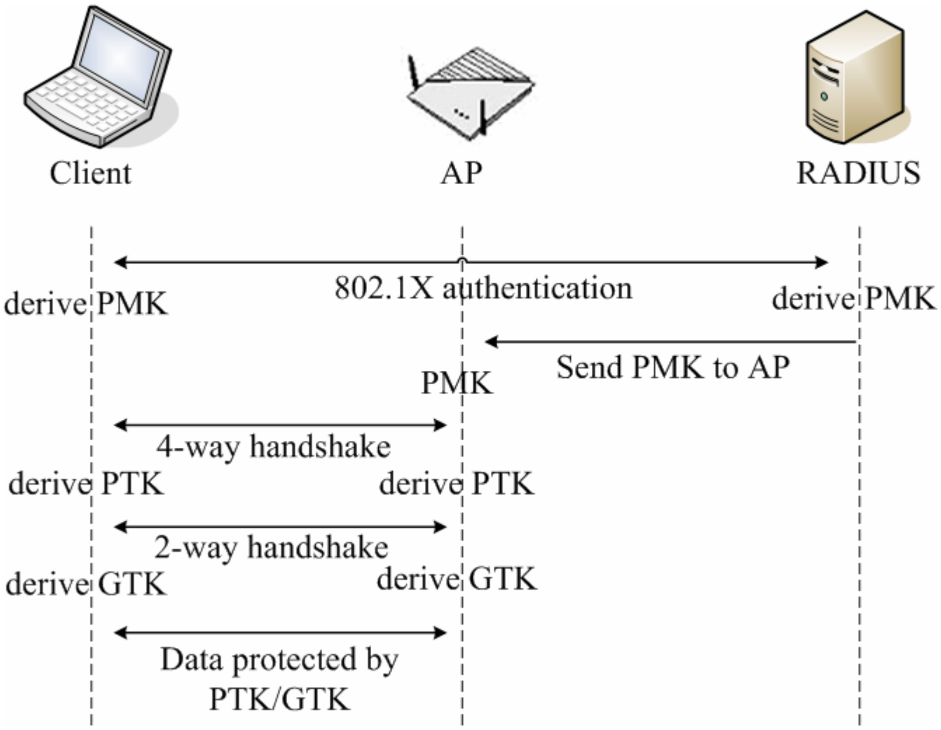


Figure 2.5 802.11i key generation

2.2 Digital certificate

2.2.1 PKI and X.509

Public key cryptography is asymmetric key cryptosystem which uses two different keys to encrypt and decrypt data. It uses public key to encrypt data and uses private key to decrypt data. Public Key Infrastructure (PKI) is based on public key cryptography and constructed by hardware, software, people and policy to provide confidentiality, authentication, data integrity and non-repudiation. [13]

X.509 is an authentication framework recommended by ITU-T. It is a part of X.500 which is a standard of electronic directory services. X.509 is based on public key cryptography and digital signatures. It defines the certificate structure and authentication protocol.

2.2.2 Digital certificate introduction

Digital Certificate is used to verify the identity of the holder of a certificate. Certificate defined on X.509 contains basic information about: Version, Serial number, Certificate issuer, Certificate holder, Validity period, Public key, Signature Algorithm, Signature. It uses public key cryptography to encrypt and decrypt data. So certificate can provide confidentiality, authentication, non-repudiation and data integrity.

The issuer of certificates is called certification authority (CA). When CA issues a certificate, it needs to sign the certificate to prove the certificate is confirmed by the CA. If a verifier trusts a CA, it also trusts the certificate signed by the CA. CA also endorses the validity of certificate, places the certificate to directory, and revoke certificate.

When user applies a certificate, he needs to generate a public key pair and submit an application to Registration Authority (RA) which is a unit to verify the data of user. There are three ways to generate the public key pair. (1) Generated by user: The private key of user is not been disclosed. But user should have the ability to generate the keys. (2) Generated by a fair third party: The fair third party should transmit the keys to user by a secure way. Then it should destroy the relative data of the keys. (3)

Generated by CA: This is the special case of (2), and CA is trusted by user.

The structure of an X.509 certificate [13]:

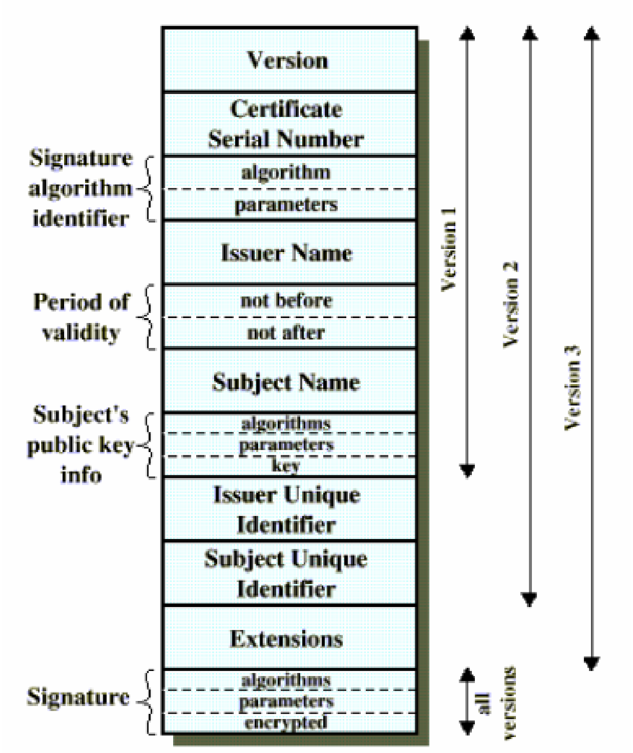


Figure 2.6 X.509 certificate

The purpose of fields:

(1) Version: The version of certificate.

(2) Certificate serial number: The unique serial number defined by CA.

(3) Signature algorithm identifier: The algorithm is used to sign the certificate by CA.

(4) Issuer name: The name of CA may include Country name, State Name, Locality name, Organization name, and Common name.

(5) Period of validity: The effective date and deadline of certificate.

(6) Subject name: The name of the holder of certificate and public key.

(7) Subject’s public key info: The value and algorithm of public key.

(8) Issuer unique identifier: Optional field. Be used to identify CA.

(9) Subject unique identifier: Optional field. Be used to identify holder.

(10) Extension: Extension field.

(11) Signature: The issuer uses its private key to encrypt above-mentioned materials and becomes the certificate signature.

Signature is used to ensure that the certificate has not been changed and indicate the identity of issuer [12]. The CA signs the certificate by using its private key. CA hashes certificate message to generate certificate digest firstly. Then CA uses its private key to encrypt the certificate digest to become certificate signature. In order to verify the validity of certificate, take the public key of issuer to decrypt the signature and check the context.

2.2.3 Certificate chain

Certificate chain is a sequence of certificates. Each certificate in the chain is signed by super-sequent certificate. The end certificate in the chain is root certificate which is self-signed. Figure 2.6 shows the relation of signed certificates in the chain.

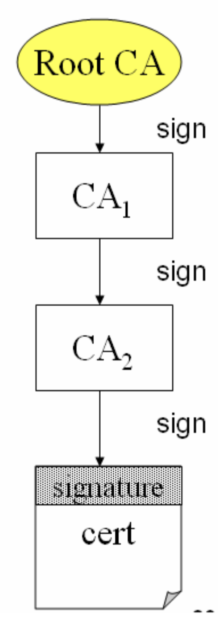


Figure 2.7 Sign certificates in chain

When a verifier wants to verify a certificate in certificate chain, it checks the CA which signed the certificate. If verifier does not trust the CA, he checks the next certificate of CA until gets a certificate of a trusted CA. And then verifier trusts the certificate which he wants to verify at the start. [13] Figure 2.7 shows the processes of verifying certificates in the chain.

The notation A<<B>> means the certificate of user B issued by certification authority A [13]. A_P means the public key of A. In Figure 2.8, if user F and user G which issued by the same CA want to verify each other and get the public key of the other side, they get the public key of CA D and certificate of each other. Then user F gets the public key of user G by $G_P = D_P D<<G>>$. User G gets the public key of user F by $F_P = D_P D<<F>>$.

When two users belonging to different CAs want to connect, they need to get the certificates and public key of super-sequence CA. In instance, user G want to verify user E, user G need to get A_P and A<<C>>, C<<E>> to do $E_P=A_P A<<C>>C<<E>>$.

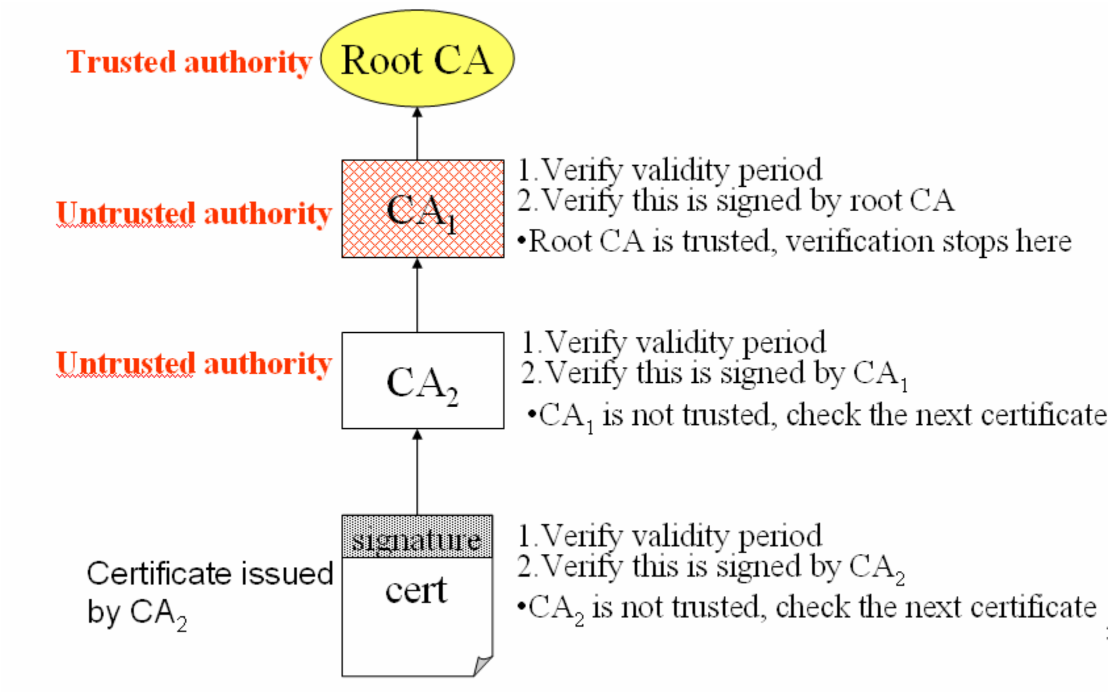

Trusted authority
Root CA
Untrusted authority
CA_1
1.Verify validity period
2.Verify this is signed by root CA
•Root CA is trusted, verification stops here
Untrusted authority
CA_2
1.Verify validity period
2.Verify this is signed by CA_1
•CA_1 is not trusted, check the next certificate
signature
cert
Certificate issued by CA_2
1.Verify validity period
2.Verify this is signed by CA_2
•CA_2 is not trusted, check the next certificate

Figure 2.8 Verify a certificate in certificate chain

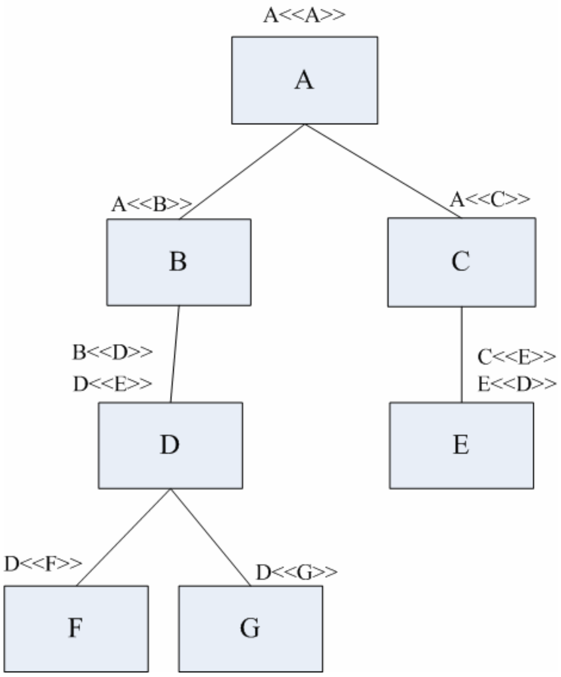


Figure 2.9 Certificate chain

2.3 Methods of fast authentication in handover

Wireless networks have already been a part of life to provide mobile communication to users. The maturity of communication techniques and services introduce ubiquitous communication and computing to mobile users. Moving between different networks or network systems without losing connection becomes a requirement of mobile communications. Handover is the process to change the network connection of ongoing call to another. Handover delay should be short enough to comply with the QoS (quality of service) requirement of mobile communications. However, authentication process in the handover procedure may spend a long time, especially when users roaming cross service domains of different operators. Therefore, improving authentication delay is necessary for achieving seamless handover. Following sections are some fast authentication methods which have been proposed include proactive key distribution, pre-authentication, fast handover method using IAPP, roaming key.

2.3.1 Proactive key distribution

Proactive key distribution intends to reduce the latency of the authentication phase by pre-distributing key material ahead of a mobile station [7]. AS creates the new PMKs of neighbor APs before MN handover. When MN moves to new AP, it derives the PMK without doing authentication.

Following are detail steps of Proactive Key Distribution:

(1) MN associates with the AP and does the authentication with AS. Then MN and AP have the PMK.

(2) The Home AS generates the new PMK from old PMK, MAC address of the

MN and of the new AP. Then AS sends new PMK to the new AP. Repeating foregoing steps for all APs in the Neighbor Graph of current (or old) AP.

(3) When the MN roams to the new AP, the MN use the same way as AS does to derive the new PMK and do key management. [8]

But there are some disadvantages of this method: (1) The AS has heavy burden for computing PMK. (2) APs cache the information (e.g. PMK) without knowing whether it will be used. This causes fat APs. (3) In order to set up neighbor graph, the network topology is known by other ISPs.

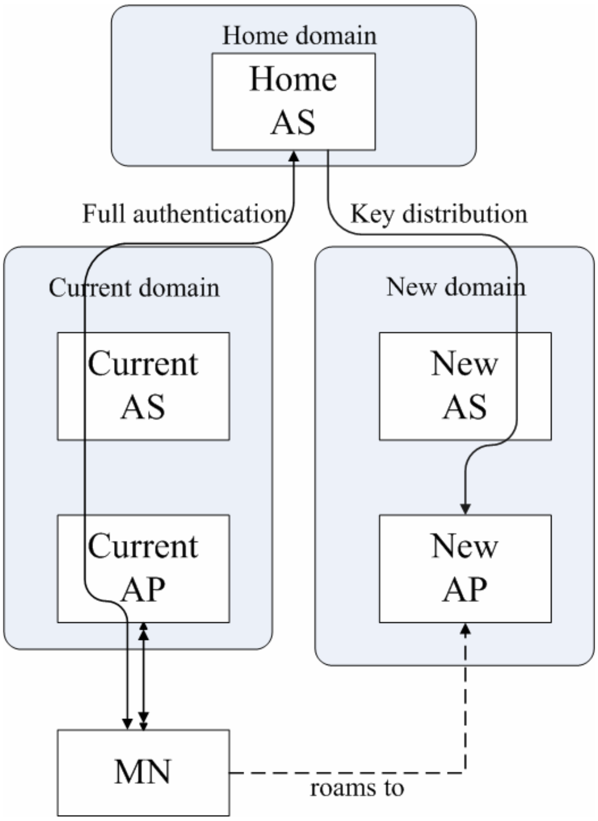


Figure 2.10 Proactive key distribution

2.3.2 Pre-authentication

IEEE 802.11i defines pre-authentication for fast roaming [8]. MN does authentication with adjacent APs before handover and caches the PMK and related information. When MN roams to AP that already did pre-authentication, it can directly do 4-way handshake.

The steps of pre-authentication:

(1) After MN associates with current AP, it sends an EAPOL-Start message to the targeted new AP which MN wants to associate later through the current AP.

(2) The new AP starts authentication with MN via the secure connection between current AP and new AP.

(3) After authentication succeeds, MN and new AP derive the new PMK, and cache it.

(4) MN roams to the AP which has done pre-authentication and do 4-way handshake directly.

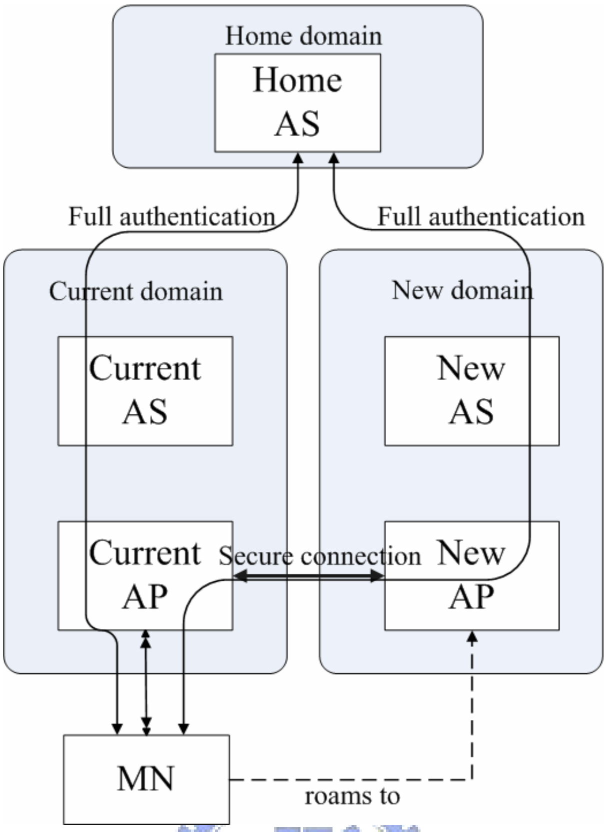


Figure 2.11 Pre-authentication

But there are some disadvantages of this method: (1) Fat APs and MNs. (2) AP needs to know the APs which adjoin it. And AP needs secure connections with adjacent APs for context transfer. (3) If new domain does not have a roaming agreement with MN's home domain, the pre-authentication will fail.

2.3.3 The fast handover method using extending IAPP

2.3.3.1 IAPP introduction

IAPP (Inter Access Point Protocol) or 802.11f is a protocol that defines the message communication between APs. IAPP can exchange the MN's security context securely between current AP and new AP during handover. The re-associate request from MN triggers the IAPP sequence between current AP and new AP. Therefore new

AP can use the context to re-associate with MN without re-authentication to achieve fast handover.

2.3.3.2 The fast handover method using extending IAPP

After full authentication, AP caches the context of MN including arguments and information about connection (e.g. PMK). When MN moves into the service region of new AP, it sends the re-associate request to new AP. Then current AP and new AP start to do the IAPP sequence as following: [16]

(1) MN sends the re-associate request includes the MAC address (BSSID) of current AP, and the ESSID and MAC address of MN to new AP.

(2) After receive the re-associate request, new AP transfers the MAC address of current AP to AS to get the corresponding IP of current AP. And new AP also gets Security Block from AS. Security Block includes the information of encryption and secret keys which are used to encrypt the messages which transmit between current AP and new AP.

(3) New AP and current AP send *Send Security Block* and *Ack Security Block* messages to ensure the Security Block context and to establish the secure connection. If the secure connection of APs has already been established before, the Security Block messages transfer can be omitted. After that both APs can encrypt the later messages exchanged between them.

(4) New AP sends MAC address of MN to current AP.

(5) Current AP verifies that the association of MN is valid, and transfers the relative context of MN to new AP and disassociate to MN.

(6) New AP sends re-associate response to MN.

(7) New AP broadcast a Link-Layer update frame to notify the Link-Layer

devices include Bridges, Switches, and AP to update the new position of MN in their forwarding tables.

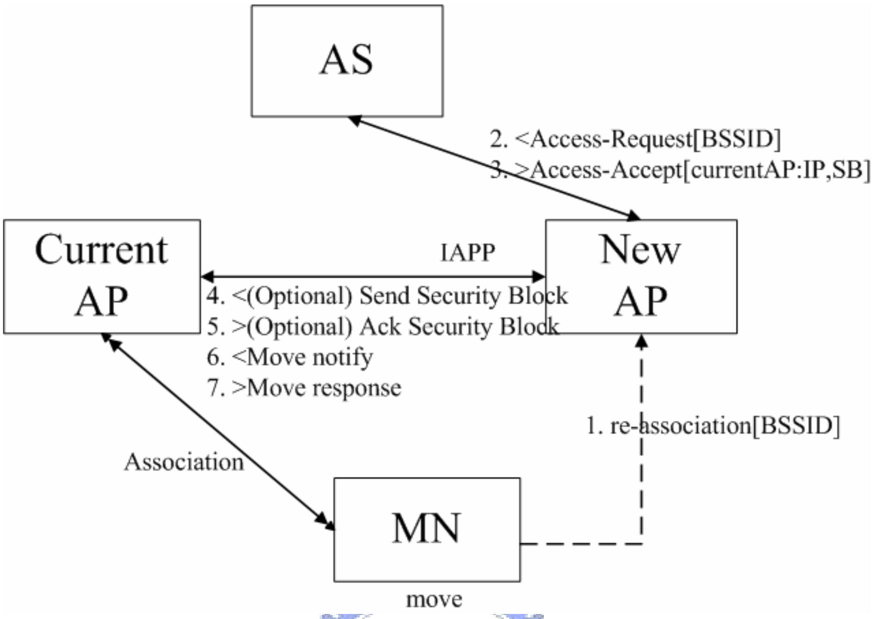

AS
2. <Access-Request[BSSID]
3. >Access-Accept[currentAP:IP,SB]
Current AP
IAPP
New AP
4. <(Optional) Send Security Block
5. >(Optional) Ack Security Block
6. <Move notify
7. >Move response
1. re-association[BSSID]
Association
MN
move

Figure 2.12 The exchanged messages in IAPP

In the inter-domain handover procedure, the IP address of AP may be a private address that hidden to the Internet. Therefore a Network Address Translation (NAT) is needed to convert the private IP addresses to public IP addresses and vice versa [8].

For secure, the context of MN sent to new AP should not contain the keys which used to encrypt the message between current AP and MN, especially during inter-domain handover. A rogue new AP may decrypt the previous traffic transmitted between current AP and MN. Therefore current AP needs to derive new keys via one-way hash function from old keys, or derives new keys regardless of the old keys.

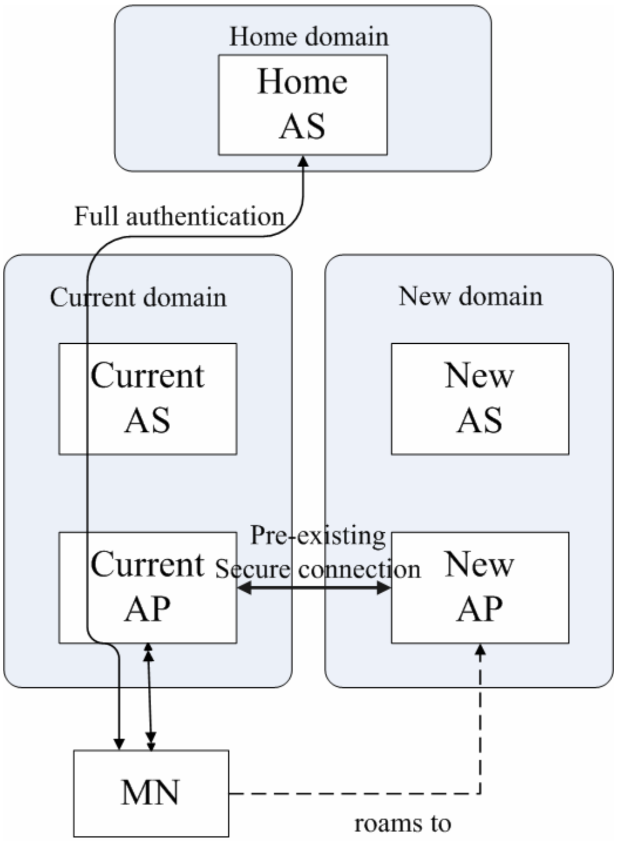


Figure 2.13 Fast handover method using extending IAPP

But there is a disadvantage of this method: The new domain may fail to do direct full authentication with home AS, because new domain does not have roaming agreement with MN’s home domain. Without re-authentication, there would have problems of overdue keys and failed validity rechecking.

2.3.4 Roaming key

A.R. Prasad and H. Wang propose “Roaming Key based Fast Handover in WLANs” in 2005. This paper proposes a Roaming Key (RK) based protocol for fast intra-domain and inter-domain handover [9]. RK is derived by PMK. It is used to provide mutual authentication between MN and new AP during handover. The roaming key mechanism is based on IAPP to transfer the context of MN between APs to achieve fast handover.

The steps of roaming key based fast handover are discussed below:

(1) After authenticate with home AS, MN and current AP derive PTK and RK from PMK.

(2) Current AP sends CI (Context Information) to neighbor APs. CI includes: PMK and its Time-Out TO_{PMK}, RK and TO_{RK}, TO_{CI}, timestamp, MAC address of AP and ID of MN (it can be a temporary ID), and encryption type.

(3) MN informs about handover to current AP. If MN would handover to different domain, current AP sends SI (Security Information) to MN. SI is information about the target network. It includes: The ESSID of target network and BSSID of AP, a new IP address of MN, the RK and an encryption key, the new PTK, and their TOs, and encryption algorithms.

(4) MN and new AP perform mutual authentication using RK and then resume communication.

(5) New AP informs home AS about handover via new AS. And MN creates new PMK, PTK and RK before the time out of RK and PTK.

But there are some disadvantages of this method: (1) Fat AP; AP caches CIs without knowing whether it will be used. (2) In order to set up neighbor graph, the network topology is known by other ISPs.

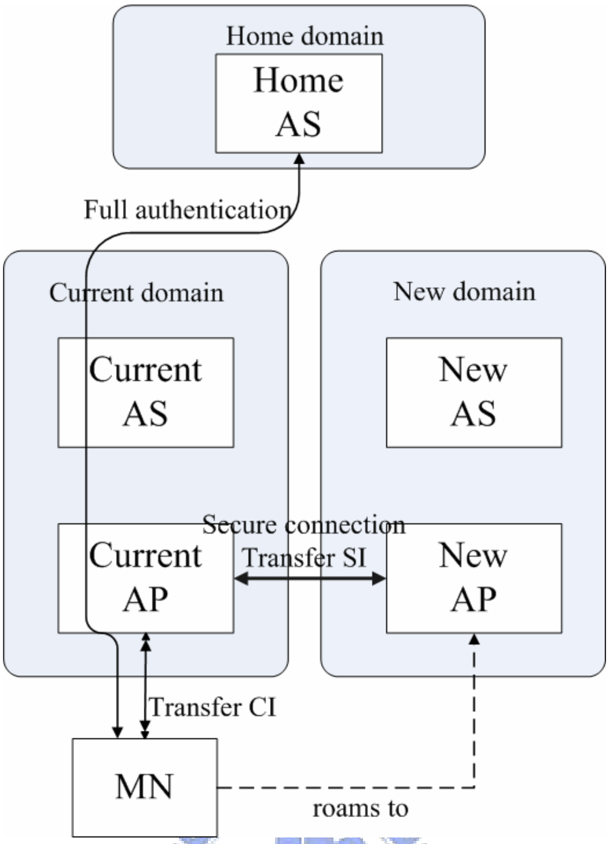


Figure 2.14 Roaming key

Chapter 3　System architecture

3.1　Wireless network environment

Wireless communications have already been a part of life. There are various wireless networks types including WLAN, 3G, MONAT, ad hot network, etc. UMTS (3G) network system is generally adopted with large-scale service area, but the communication cost is still high. On the other hand, the coverage of WLAN is small but the transmission rate is high with low communication cost. From the perspective of efficiency and economy, WLANs can be taken as the complementary network system of the ubiquitous 3G mobile communication system. An operator may establish 3G networks and WLAN simultaneously. The networks that are owned by the same operator belong to the same trust domain. Assume that there is a Master Operator (MO) in an area. The amount of MO's subscribers predominates over the amount of mobile users in an area. The other operators in this area would cooperate with the MO to complement the coverage of service region. MOs of different areas or countries may cooperate with each other to provide roaming services. If the MO in area A has cooperation with the MO in area B, the operator in area A and the operator in area B can have implicitly trusted relation through MOs.

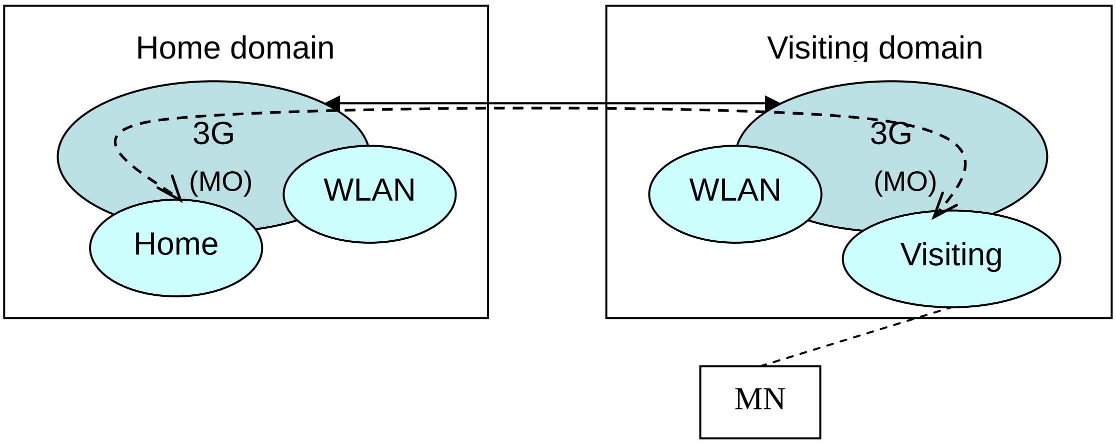


Figure 3.1 Wireless network environment

3.2 System targets

The liberty and legislation of telecommunications encourage the investment of more operators to join the market. The construction of trust relations of various service domains becomes more complicated when more networks are involved in the communications environment. Implementing a fast authentication method in above-mentioned environment should have some characteristics: (1) Visited domain has no need to cooperate with MN’s home domain, thus can minimize the direct roaming agreements. MN can roam to a domain without roaming agreement with its home domain. (2) Visited domain can demand full re-authentication with MN. In order to ensure proper accounting or validity of peers, re-authentication is required.

However, current fast-authentication methods which discussed in chapter 2.3 can not fulfill these requirements simultaneously. Therefore we propose a novel fast-authentication mechanism to reduce the authentication delay in inter-domain handover without requiring mutual roaming agreement of mobile operators.

3.3 System concept

The system that we propose bases on IAPP to communicate and transfer context between current AP and targeted AP when MN inform about handover. When MN firstly visits a new domain, the visited domain needs to query the MN's home domain to authenticate the visiting MN. If the visited domain has roaming agreement with MN's home domain, MN can do full authentication with home domain via visited domain. After authentication AP caches the relevant context of MN including arguments and information about connection. When MN wants to roam from current AP to new AP, it sends a re-association request to new AP. New AP receives the request, and sends a request to current AP. Then current AP sends the relevant context of MN to new AP. New AP uses the context to re-establish connection with MN without doing authentication and setting up the connection information again. Therefore handover latency can be reduced to comply with the QoS requirement of mobile communications.

After the handover, re-authentication would be required when secure keys are overdue or AP or MN wants to recheck the validity of the other side. The fast handover method using extending IAPP which is discussed in chapter 2.3.3 can do the re-authentication if visited domain and MN's home domain do not have cooperation. It would be a serial secure problem in roaming. In order to solve this problem, this thesis proposes a one-hop re-authentication method. MN and AP have their certificates issued by trusted CA. They use the certificates to do re-authentication using EAP-TLS. Because the authentication is only between MN and AP and different to traditional authentication, it is called one-hop authentication.

3.4 System scenarios

This section discusses the scenarios and authentication procedures of the proposed method.

3.4.1 Domain relation and certificate chain

With the environmental assumption in the chapter 3.1, there would have a MO in an area. The MO cooperates with the other operators in the area to extend the coverage of service region. Because the MO is a trusted third party for the other operators, the MO of an area can act as the root CA to issue certificates to the ASs of the operators which have roaming agreement with MO. Then AS issues certificates to APs of its service domain. Hence, starting from the root CA, a certificate chain is established among MO, AS and AP of the same communication network.

Two certificates issued by the same root CA imply a trust relation by verify the certificates of each. Only when the MO and the domain have roaming agreement or trust relation, the root CA issues a certificate to the domain. By trusting the MO as a root CA, when domain A successfully verifies a certificate of domain B which issued by the same root CA, domain A can trust domain B as valid. Then a trust relation is established between the two domains. Accordingly to the concept of certificate chains, the trust relations can be dynamically established between different domains.

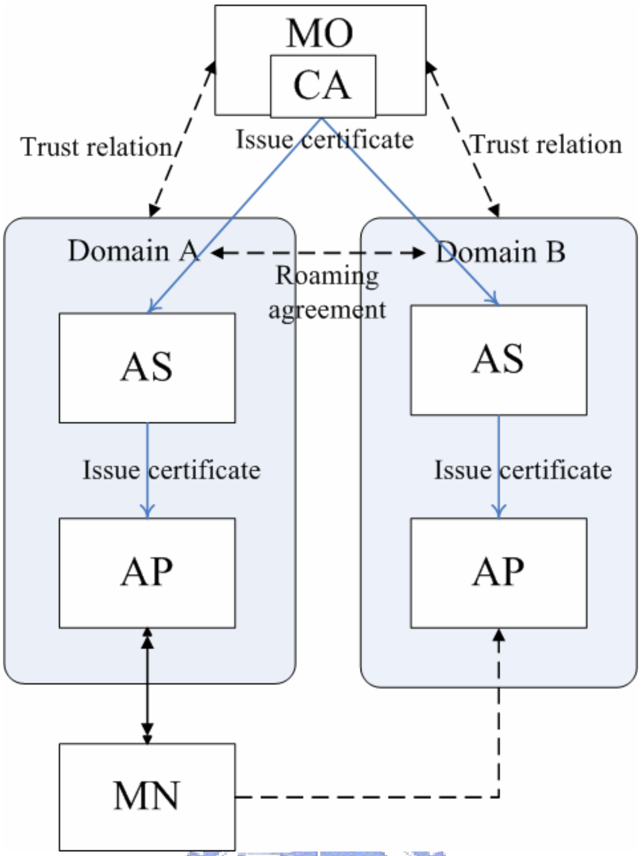


Figure 3.2 Domain relation and certificate chain

MOs in different areas may have roaming agreement to allow user mobility between the two communication domains. When MOs have roaming agreement, they issue the certificates to each other to connect the two certificate chains of each network domain. As shown in Figure 3.3, MO_1 has the certificates issued by MO_1 and MO_2, and MO_2 has the certificates issued by MO_2 and MO_1. When AS_B wants to verify AS_C, it follows the chain to get 2<<C>> and 1<<2>>. MO_1 is the trusted authority of AS_B, so the verification started from AS_B will stop at MO_2 and come out a positive result. The detail process of verification is depicted as:

$2_P = 1_P 1<<2>>$, $C_P = 2_P 2<<C>>$, *verify successfully.*

On the other hand, AS_C verifies AS_B in the same way. After verified the certificates, a trust relation is established between AS_B and AS_C.

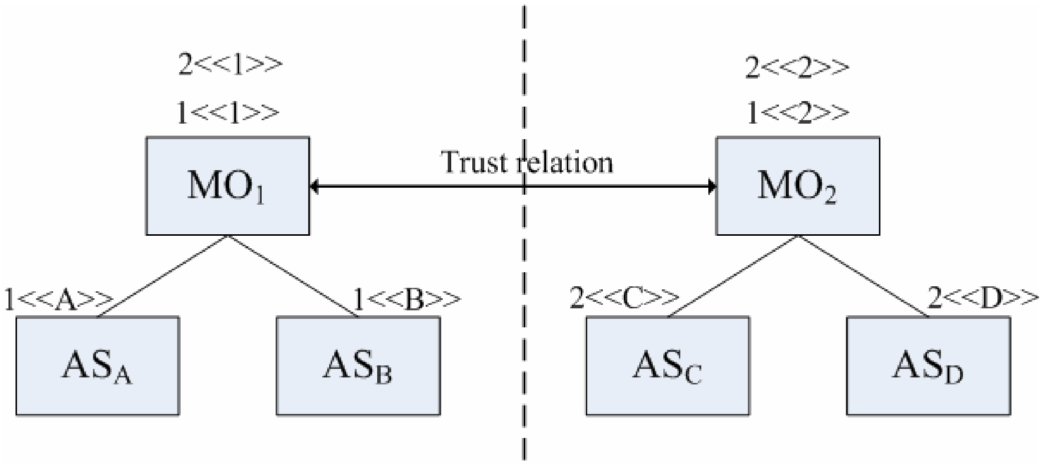


Figure 3.3 Establish trust relation across different MOs

3.4.2 Register in home domain

Before MN accessing a wireless networks, it should register to a domain and get a certificate from AS. MN may also cache the certificates of domains which have roaming agreement with its home domain.

3.4.3 Visit a network

When MN is turned on and visits a domain, it should do authentication with its home domain to confirm validity. If MN visits a non-home domain, the roaming agreement between visited domain and MN's home domain needs to be checked. If there is no roaming agreement between them, two domains use the certificate chain verification to determine that the other domain can be trusted or not. After certificate chain verification succeeds, the trust relation and roaming agreement are established between the domains. We particularly discuss the visiting situations and the corresponding processes of them below.

A. If MN visits its home domain

1. MN do full authentication with AS via AP.
2. After authentication succeeds, AP caches context information including PMK, and certificate of AS. MN caches context information including PMK, and certificate of root CA_{Home}.

B. MN visits a domain which has roaming agreement with MN's home domain

1. MN do full authentication with home AS via AP.
2. After authentication succeeds, AP caches context information including PMK, and certificate of MN's home AS. MN caches context information including PMK, and certificate of root CA_{Visit}.

C. MN visits a domain which has no roaming agreement with MN's home domain

1. If the visited domain and home domain trust the same root CA or they trusted CAs trust each other such as the AS_A and AS_C in Figure 3.3. Two domains do certificate verification firstly to establish the trust relation between each other.
2. MN do full authentication with home AS via AP.
3. After authentication succeeds, AP caches context information including PMK, and certificate of MN's home AS. MN caches context information including PMK, and certificate of root CA_{Visit}.

3.4.4 Handover processes

When MN moves to the range of new AP and wants to re-associate with the new AP, it sends a re-associate request message to new AP. The following discusses the situations of roaming and corresponding processes.

A. Roam to the same domain as current AP. Or roam to a new domain that has cooperation with current domain.

(1) MN sends a re-associate request to the new AP includes the MAC address of current AP, and the ESSID and MAC address of MN.

(2) New AP sends MAC address of current AP to AS to get the IP address of current AP. If the secure connection has not been established, transfer the Security Block messages firstly.

(3) New AP sends MAC address of MN to current AP in order to verify that the association of MN in current AP is valid or not.

(4) Current AP transfers MN’s relevant context including PMK, and certificate of MN’s home AS to new AP.

(5) New AP sends re-associate response to MN.

B. Roam to a new domain which does not have cooperation with current domain.

If the new domain and current domain both have cooperation with the same MO and have certificates issued by the same root CA, or they in different MO but their cooperating MOs have roaming agreement, the new domain and current domain do certificates verification to establish trust relation. After the above-mentioned processes, do the processes as situation *A* which discussed before does.

However, if the new domain can not establish a trust relation with current domain but has a roaming agreement with MN’s home domain, MN does a full authentication with its home domain via new domain.

After re-association succeeds, current AP becomes old AP and new AP becomes current AP.

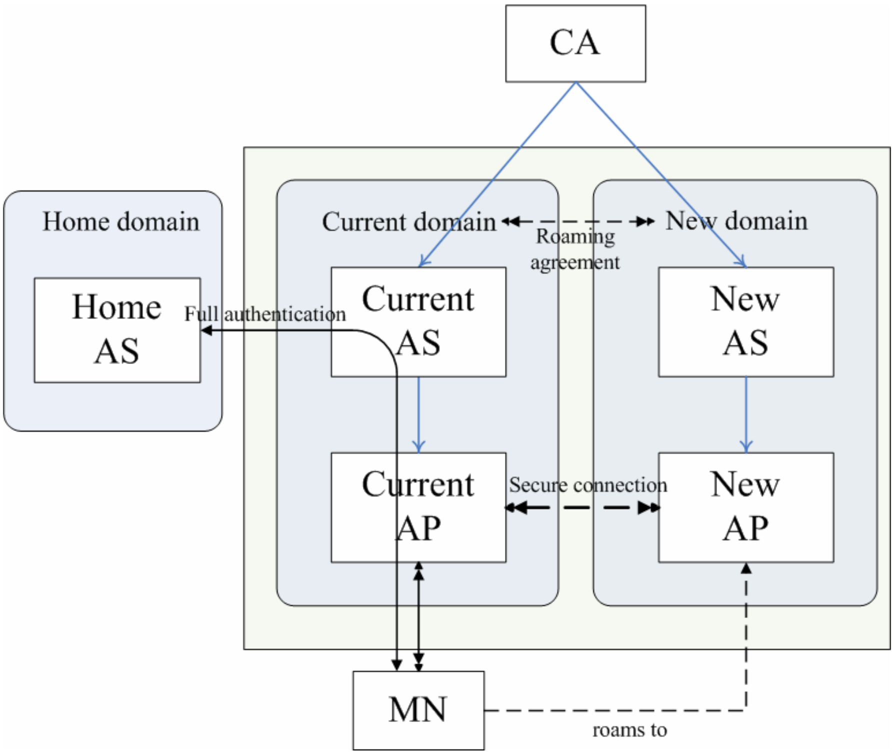


Figure 3.4 Handover processes

3.4.5 One-hop re-authentication

When the keys become overdue or AP or MN wants to recheck the validity of the other side, the re-authentication is needed. But the new visiting domain may not have roaming agreement with MN's home domain in inter-domain roaming. MN can not do authentication with its home domain directly. It would be a serial secure problem in roaming. Therefore we propose a one-hop re-authentication to let MN and AP can verify each other without relying on AS.

MN and AP use certificates to do EAP-TLS full authentication. MN has certificate issued by its home AS. AP has certificate issued by AS. When MN visited the old domain, it got the certificate of CA_{Visit} which is the root CA of visited domain. MN verifies the certificate of current AP by certificate of CA_{Visit} via certificate chain. The certificate of current AP is signed by current AS which is not trusted by MN, therefore MN check the next certificate. The certificate of current AS is signed by CA_{Visit} which is trusted by MN. Therefore, MN uses the public key of CA_{Visit} to verify the signature in the certificate of current AS which is signed by the private key of CA_{Visit}. And then MN uses the public key of current AS to verify the signature in the certificate of current AP. After verification succeeds, MN can be sure the AP is valid and is trusted by the CA_{Visit}. In the other hand, AP verifies the certificate of MN by the certificate of MN's home AS which is transferred from old AP via IAPP in the same way as above-mentioned.

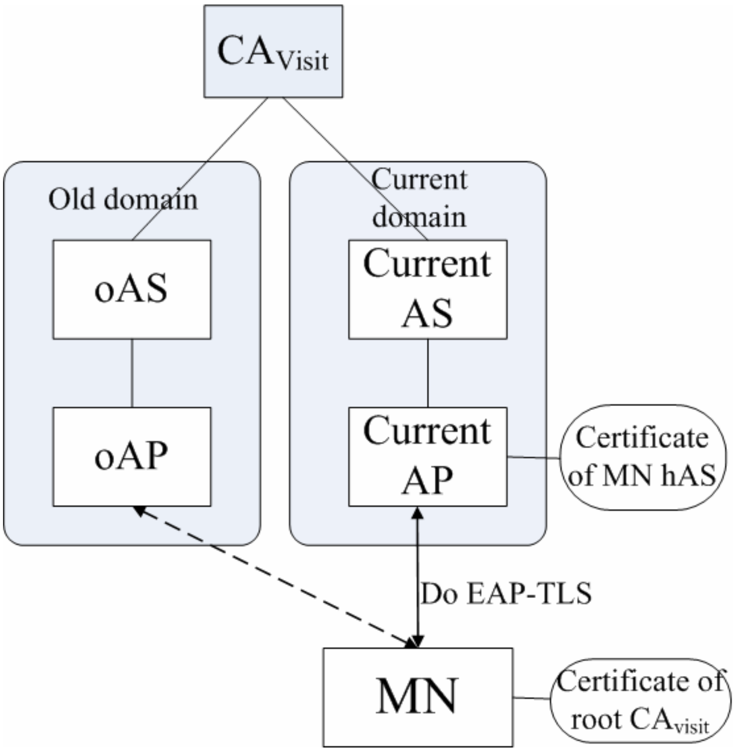


Figure 3.5 One-hop re-authentication

Chapter 4 Analysis and Comparison

4.1 Analysis

Based on extended IAPP we proposed a fast handover mechanism. The proposed mechanism has the properties of:

(1) Fast handover;

(2) Requirement of roaming agreement;

(3) Dynamic trust relation;

(4) Capability of re-authentication;

(5) Reduce burden of AS;

(6) Based on present protocol;

(1) Fast Handover:

Our method is based on IAPP to do fast handover. When MN wants to handover, current AP transfers the context of MN to new AP. New AP uses the context to establish connection with MN without authentication with AS again to reduce the authentication delay. [14] mentioned that the overall latency in layer 2 and layer 3 should not exceed 50 ms to prevent excessive jitter. Fast handover using IAPP can reduce the handover delay to an average 15.37 ms.

When the new domain has no roaming agreement with visited domain, the two domains need to do certificate verification and establish roaming agreement firstly that can bring about roaming delay. However, the trust relation of the two domains is established during the process of certificate verification, if the other MN wants to handover between these two domains afterward, they can do IAPP processes directly without extra verification delay between domains.

(2) *Requirement of roaming agreement:*

Most methods need to do authentication with home domain during handover. MN can only access the network domain which has roaming agreement with the MN’s home domain. In actual environment, domains which are located in different areas unlikely have roaming agreement with each other. A domain usually has roaming agreements with neighboring domains to extend the service range. Therefore, the domains an MN can visit are limited and the range an MN can visit is restricted by using the former methods.

Our proposed method is based on extending IAPP which has characteristic that an MN can visit a domain without roaming agreement with the MN’s home domain. MN and the new domain establish an implicit trust relation via the visited domain which adjoins the new domain. Via the trust relation between the visited domain and other domains, the trust relation is implicitly implied to the MN’s home domain, thus an MN can roam to other domains..

(3) Dynamic trust relation:

If the new domain that MN wants to connect has no roaming agreement with the visited domain nor the MN’s home domain, the connection will be refused. Our method provides the certificate chain verification mechanism to dynamically establish the trust relation between domains. Each domain has its certificate. When domain A wants to verify whether the certificate of domain B is valid, domain A checks the CA which signed the certificate of domain B. If domain A does not trust the CA, it checks the next CA in the certificate chain until meets a trusted CA. Then domain A trusts that the certificate of domain B is valid and domain B is trustable.

(4) Capability of re-authentication:

Based on the concept of certificate chain, we propose one-hop re-authentication to overcome the shortcoming of extended IAPP-based fast handover methods that can not perform re-check if new domain has no roaming agreement with home domain. The one-hop re-authentication method establishes trust relations of domains via certificate chains, and uses the EAP-TLS for full authentication between MN and AP to verify the validity of peers and generate a new secret key PMK. This method allows MN roaming between different network domains without worrying about the security.

(5) Reduce burden of AS:

When MN moves to the service region of a new AP, it needs not to execute the authentication process to establish a trust relation between itself and the AP. This method can alleviate the computing effort of AS and enhance the roaming efficiency.

(6) Based on present protocol:

The method we proposed is developed on the existing protocols including IAPP, certificate chain, EAP-TLS. Therefore the implementation of the proposed method requires neither the modification of existing protocols nor the upgrade of network facilities.

4.2 Comparison

In this section we compare the proposed mechanism with existing fast handover method to prove the feasibility and the advantages of our mechanism.

(1) Roaming agreement relation:

The fast handover methods include proactive key distribution, pre-authentication and roaming key. All the mentioned mechanisms require that the domains which MN roams to need to have roaming agreement with the MN's home domain. In other words, MN using those methods can not roam to the domains without cooperation with the MN's home domain.

The method using extending IAPP and the method we proposed can roam to the domains do not have roaming agreement with home domain. Because MN and the new domain have implicit trust relation between them via the trust relation in visited domain.

(2) *Re-authentication is available in the visiting domain:*

The fast handover methods include proactive key distribution, pre-authentication, and roaming key can do re-authentication because visited domains need to have roaming agreement with home domain.The method using extending IAPP can not do re-authentication directly. Therefore, the method we proposed utilizes the properties of certificate chain to add the one-hop re-authentication mechanism to enable re-authentication between MN and AP.

Table 4.1 shows the result of comparing our proposed method, proactive key distribution, pre-authentication, methods using extending IAPP and roaming key in direct agreement and re-authentication.

Items Methods	Without direct agreement	Re-authentication
Proposed method	Yes	Yes
Proactive key distribution	No	Yes
Pre-authentication	No	Yes
Methods using extending IAPP	Yes	No
Roaming key	No	Yes

Table 4.1 Comparison

Table 4.1 shows our proposed method can make MN to roam to a domain without direct agreement with MN's home domain and can do re-authentication in the visiting domain. The proposed methods fulfill all the requirements of fast authentication.

Chapter 5　Conclusion

Nowadays, wireless network is more important in our life, and mobility becomes a basic requirement for users. Achieving seamless handovers across networks and domains becomes an important topic for discussion. This thesis discusses the methods of reducing authentication delay to shorten handover delay effectively. Besides reducing the authentication delay, the basic authentication requirements still exist. We propose a method which is based on IAPP and uses certificates chain to do one-hop re-authentication. Current AP and new AP transfer the context of MN during handover. New AP uses the context to establish connection with MN without authentication with AS again to reduce the authentication delay. After establishing the connection, there exists an implicit trust relation between MN and AP. The one-hop re-authentication let MN and AP use certificates to verify each other and establish an explicit trust relation.

We also consider the relationship among domains. Neighboring domains often establish roaming agreements to extend service region. Therefore our method allows MN to roam to a new domain which does not have roaming agreement with the MN's home domain which may locate far from the new domain. The new domain only needs to have roaming agreement with the MN's visited domain that adjoins the new domain. Even if MN wants to connect the new domain that has no roaming agreement with visited domain, our method provides the certificate chain verification to dynamically establish the trust relation between domains. Such that an MN can move to anywhere without wondering the roaming boundary.

References

[1] P. Congdon, B. Aboba, A. Smith, G. Zorn and J. Roese, “IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines” RFC 3580, September 2003

[2] Bernard Aboba, Tim Moore, John Roese, Ravi Nalmati, Albert Young, Carl Temme, Bill McFarland, David Halasz, Paul Congdon, Andrew Smith, “IEEE 802.1X For Wireless LANs” IEEE 802.11, March 2000

[3] C. Rigney, S. Willens, A. Rubens, W. Simpson, “Remote Authentication Dial In User Service (RADIUS)” RFC 2865, June 2000

[4] C. Rigney, “RADIUS Accounting” RFC2866, June 2000

[5] W. Simpson, “The Point-to-Point Protocol (PPP)” RFC1661, July 1994

[6] D. Simon, B. Aboba, R. Hurst, “The EAP-TLS Authentication Protocol” RFC 5216, March 2008

[7] Arunesh Mishra, Min Ho Shin, William A. Arbaugh, “Pro-active Key Distribution using Neighbor Graphs” University of Maryland

[8] M.S. Bargh, R.J. Hulsebosch, E.H. Eertink, A. Prasad, H. Wang, P. Schoo, ”Fast Authentication Methods for Handovers between IEEE 802.11 Wireless LANs” WMASH’04, October 2004

[9] A.R. Prasad, H. Wang, “Roaming Key based Fast Handover in WLANs” IEEE, 2005

[10] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, “Extensible Authentication Protocol (EAP)” RFC 3748, June 2004

[11] 陳哲儀 “行動網路技術 WLAN 安全性” 元培大學

[12] Security Overview, Digital Certificates, http://developer.apple.com/documentation/Security/Conceptual/Security_Overview/C

oncepts/chapter_3_section_7.html

[13] William Stallings, “Cryptography and Network Security Principles and Practices” 3rd Edition, Prentice Hall, 2003

[14] Arunesh Mishra, Min-ho Shin, William, A. Arbaugh, “Context Caching using Neighbor Graphs for Fast Handoffs in a Wireless Network” IEEE, 2004

[15] 簡榮宏, 黃玉佳 “基於 IEEE 802.11i 的快速預先認証” 交通大學

[16] 高授樹 “802.11 無線網路漫遊系統整合與分析” 大葉大學, 2005