行政院國家科學委員會專題研究計畫　期中進度報告

子計畫四：快速行動擷取網路中之品質服務支援技術研究

(2/3)

計畫類別： 整合型計畫
計畫編號： NSC93-2213-E-009-052-
執行期間： 93 年 08 月 01 日至 94 年 07 月 31 日
執行單位： 國立交通大學資訊工程學系(所)

計畫主持人： 陳耀宗

計畫參與人員： 林政豪 許銜書 林雋永

報告類型： 精簡報告

處理方式： 本計畫可公開查詢

中　華　民　國 94 年 5 月 31 日

行政院國家科學委員會補助專題研究計畫 □ 成 果 報 告 □期中進度報告

支援下一代無線與 FTTx 擷取之光纖都會網路技術—子計畫四：快速行動擷取網路中之品質服務支援技術研究
QOS Enabling Technology for High Mobility Wireless Network

計畫類別：□ 個別型計畫　　☑ 整合型計畫
計畫編號：NSC －93 － 2213 － E － 009 － 052
執行期間： 93 年 8 月 1 日至 94 年 7 月 31 日

計畫主持人：陳耀宗
共同主持人：
計畫參與人員： 林政豪 許銜書 洪立哲 林雋永

成果報告類型(依經費核定清單規定繳交)：☑精簡報告　□完整報告

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、列管計畫及下列情形者外，得立即公開查詢
□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：國立交通大學資訊工程學系

中 華 民 國 九十四 年 六 月 十四 日

「支援下一代無線與 FTTx 擷取之光纖都會網路技術」子計畫四
「快速行動擷取網路中之品質服務支援技術研究」
QOS Enabling Technology for High Mobility Wireless Network

計畫編號：NSC 93-2213-E-009-052
執行期限：93 年 8 月 1 日至 94 年 7 月 31 日
主持人：陳耀宗教授　(國立交通大學資訊工程學系)
計畫參與人員：林政豪 許銜書 洪立哲 林雋永

一、中文摘要

隨著無線網路的迅速發展，有許多相關的議題也開始被探討。目前可攜式無線裝置在網域間漫遊的服務，可透過快速交遞(Fast handover)與階層式 Mobile IP (Hierarchical Mobile IP)，來降低可攜式無線裝置在交遞的過程中，封包遺失率與交遞遲滯等問題。當可攜式無線裝置在交遞過程中，除了完成交遞步驟外，也由於採取認證機制，會使得可攜式無線裝置，因認證機制的複雜程度，間接拉長了整體的交遞時間，使得可攜式無線裝置無法迅速重新取得資料，造成封包遺失，因此降低服務品質。目前認證機制的方法有相當多的架構被提出來，包括 AAA(Accounting, Authentication, Authorization)、IEEE 802.1X…等。每種方法的複雜程度不一樣，所影響的程度也不同。在本篇報告中，我們提出一個二階段式的低遲滯交遞認證機制，讓可攜式無線裝置在即將漫遊前，將一些認證資訊藉由快速交遞協定，提前帶給即將前往的路由器認證，並取得臨時通行憑證與正式憑證，使得可攜式無線裝置能到新的網域下，藉由此臨時通行憑證，迅速接收資料。同時可攜式無線裝置在發出臨時通行憑證後，必須在規定的時間內，送出正式憑證，以完成正式的認證。透過 ns-2 程式的模擬，我們驗證了此機制的效能，證明隨著資料量的增加，更能突顯提前認證的效能與重要性。

關鍵字：低遲滯交遞機制；提前認證；臨時通行憑證；正式憑證

二、英文摘要

With the rapid growth of wireless networks, many related topics have been proposed and discussed. Currently, the combination of Fast Handover and Hierarchical Mobile IP can reduce the packet loss rate and handover time problems of mobile devices roaming between subnets. During the handover period, a mobile device needs to perform fast handover signaling as well as authentication mechanisms. The total handover latency and packet loss rate of mobile device will increase according to the complexity of the authentication mechanism. This negative impact causes mobile devices unable to transmit its real-time data packets promptly, hence degrade the quality of services. Several authentication methods such as AAA (Accounting, Authentication, Authorization) and IEEE 802.1x have been proposed. The complexity of these methods still cannot fulfill the QoS requirement of certain real-time traffic. We propose a two-stage authentication scheme in this project for achieving low-latency handoff. It allows mobile devices to send certain authentication information by fast handover protocol to obtain a temporary certificate from new access node before roaming to the new domain. A mobile device can use the temporary certificate to receive real-time data packet quickly and then perform formal authentication process by sending the formal certificate to complete the total authentication as normal procedure. We evaluate the performance of the proposed method by using ns-2 simulator and it demonstrate that pre-authentication scheme really improve the quality of services during the handover process.

Keywords: pre-authentication, temporary certificate, formal certificate, low latency

三、計畫緣由與目的

Wireless local area networks have become extremely popular in recent years. The wireless services may encounter some problems under different environments, and there are more emerging multimedia streaming applications being developed.

When users of these applications move from the coverage area of one AP to the other, the services must be handed over in approximately 150 milliseconds, otherwise the user will experience the jitter. If the handoff time is much larger than 150ms, the quality would be getting worse. This noticeable problem needs to be solved. Many approaches have been proposed from different aspects to reduce the handoff impact. Some focus on layer2 handoff to reduce the scan, authentication and association latency. Others focus on layer 3 handoff to alleviate the registration and authentication time. The typical solution for reducing handoff time is Hierarchical Mobile IP with Fast handover protocol. Fast handover protocol needs layer2 information to early trigger the handoff and it spends approximately 100ms which is much smaller than 3 seconds required by original Mobile IP. This small handoff period allow us to provide a multimedia streaming service during handoff without suffering jitter problem.

Besides handoff, security and authentication issues also become more important nowadays. If we like to enhance the security or to perform authentication, it will add a certain amount of handoff time in addition to the original layer2 and layer3 handoff. This is a tradeoff between authentication and QoS, and we need some method to minimize the impact if we add authentication process on it. Fast handover could provide better QoS for roaming devices, based on this advantage, we construct a user authentication signaling that allows the access router to authenticate the mobile node(MN). Here, we propose a pre-authentication scheme based on fast handover signaling to pre-authenticate the roaming device before the formal handoff process starts. It tends to perform original fast handover protocol without authentication, and we called it the two-stage authentication scheme.

四、研究方法與成果

To achieve low latency handoff, we make use of pre-registration signaling called fast handover protocol to piggyback user's information to authenticate with new target AP temporarily for reducing the authentication time during handoff period, it is called "two-stage authentication". Our two-stage authentication scheme consists of pre-authentication and formal authentication. A mobile node needs to perform AAA/Mobile IP initial registration when it enters into the new MAP (Mobility Anchor Point) domain. The Home Agent generates keys and authenticates the mobile node when it receives the AAA/Mobile IP registration message. Then, the Home Agent replies the registration to the mobile node through MAP, which then checks the authentication status, signs a certificate CA_{MAP} and adds group key for the mobile node into registration reply message as shown in Figure 1.

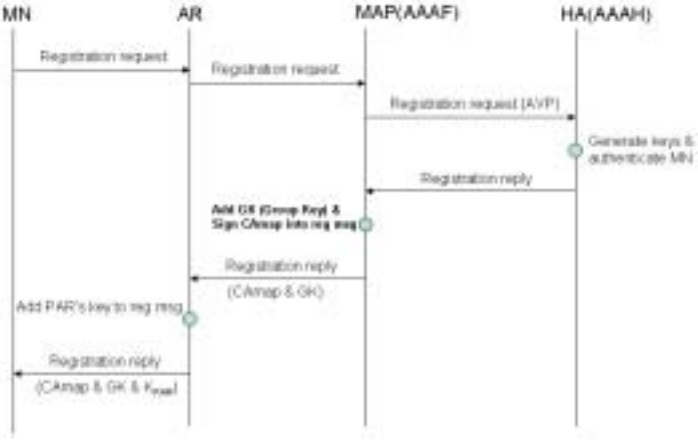

Figure 1 CA_{MAP} & GK & Key_{PAR} distribution flow

The mobile node derives the CA_{MAP} after performing the AAA/Mobile IP registration. Then, the mobile node moves from PAR (Previous Access Router) to NAR (New Access Router), it triggers the pre-registration called fast handover signaling to reduce the registration time. We try to make use of this signaling to piggyback some information to pre-authenticate the MN with new target AP temporarily. Also, the MN needs to complete the formal authentication process after handoff in a given limited time. The information in fast handover signaling is presented in Figure 2.

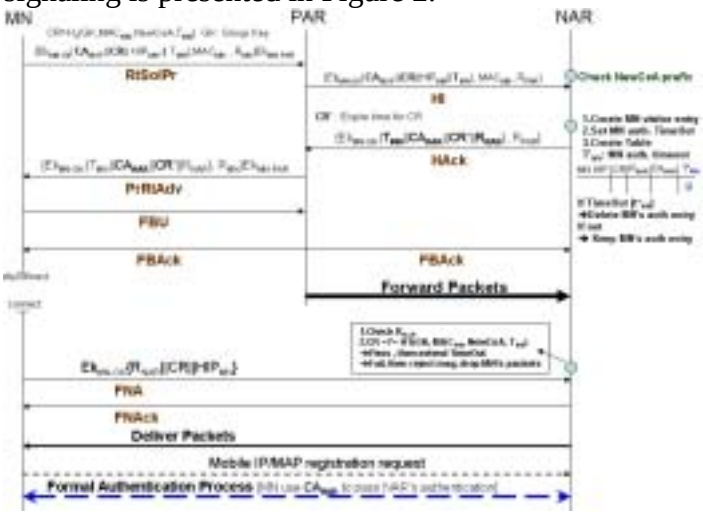

Figure 2 Pre-authentication messages in fast handover

The MN generates a credential to register with new target AR (AP) through fast handover signaling

for deriving the temporarily access right in the new domain. After handoff, the mobile node can receive packets quickly by sending this credential to the target AR to present its existence under target AR's coverage. So, the MN doesn't need to wait for completing the authentication process to receive packets. Figure 3 shows the pre-authentication messages in fast handover signaling. NAR uses CA_{MAP} to identify the mobile node and to register the credential of the mobile node in NAR's authentication table. NAR will return the expiration time of the credential and CA_{NAR} signed by NAR through fast handover signaling to the mobile node. After Layer 2 handoff, the MN can use this credential to pass temporarily authentication and extend its authentication expiration time in NAR's authentication table. CA_{NAR} is for formal authentication usage.

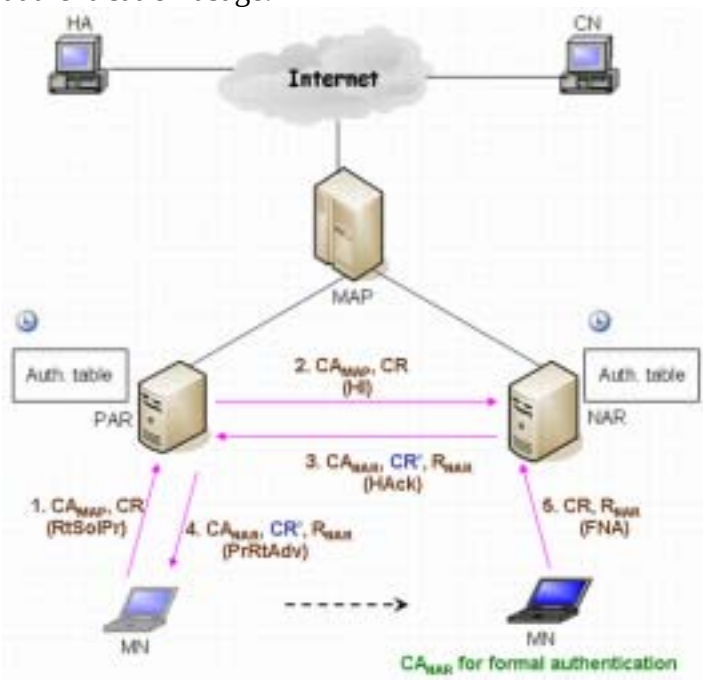

Figure 3 Pre-authentication message flow

NAR uses CA_{MAP} to sign a new certificate CA_{NAR} to the MN for formal authentication process. The MN needs to send this CA_{NAR} to NAR to pass the formal authentication before the credential expires. So, it needs 4-way handshaking to complete the authentication steps as shown in Figure 4. If the MN derives the CA_{NAR}, it just needs 2 way handshaking to send the CA_{NAR} to update its authentication status in NAR periodically. Then, we compare our scheme with L3-FHR authentication approach as shown in Figure 5 and Figure 6.

L3-FHR broadcasts authentication reply packets to all L3-FHR APs (ARs). So a MN can re-authenticate with new target AP without authenticating with home AAA server again. It may reduce the re-authentication time. New target AP will stop dropping packets after MN completes the re-authentication.

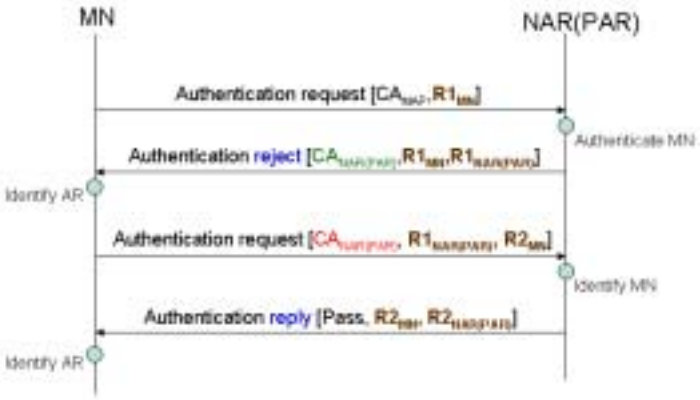

Figure 4 The 4-way formal authentication

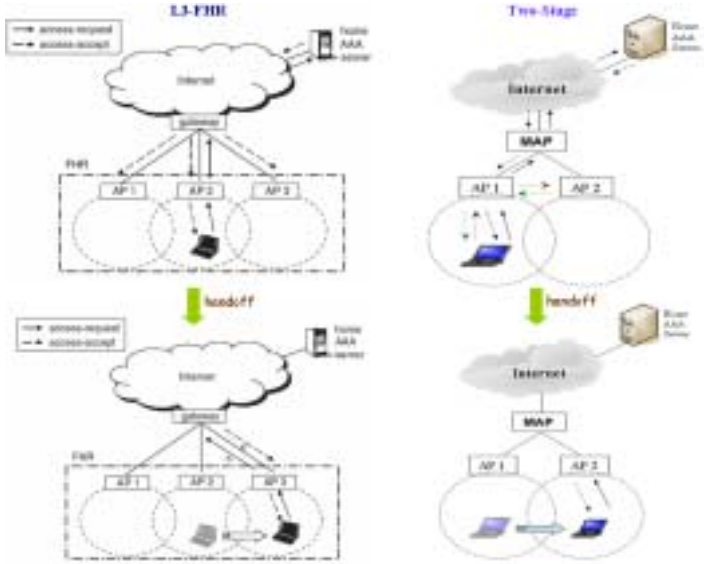

Figure 5 L3-FHR & Two-Stage message flow

	L3-FHR	Two-Stage
Main idea	Pre-send auth. info to target APs	Pre-send auth. info to target AP
How to pre-send (Method)	Through L3-FHR	Through Fast handover signaling
Initial authentication	Register and authenticate with Home AAA server	Register and authenticate with Home AAA server
When to pre-send	BW receives auth. info. duplicates it to all L3-FHR APs	MN just sends auth. info to target AP by fast handover before L2 handoff
When to authenticate with new AP	MN re-authenticates with new target AP when it moves to target AP after L2 handoff	a. Before L2 handoff, MN pre-authenticates with new target AP temporarily. b. After L2 handoff, MN performs formal auth. with new target AP
When to stop dropping packets	MN completes the re-authentication with new AP after L2 handoff	MN completes the pre-authentication with new AP before L2 handoff
When to delete authentication information	MN doesn't authenticate with that AP before its timer expires	MN doesn't authenticate with that AP before its timer expires

Figure 6 L3-FHR & Two-Stage Comparisons.

Both these two schemes pre-send the authentication information to the new target AP before handoff. But the two-stage scheme not only pre-sends this authentication information but also registers its

authentication information temporarily with new target AP before L2 handoff.

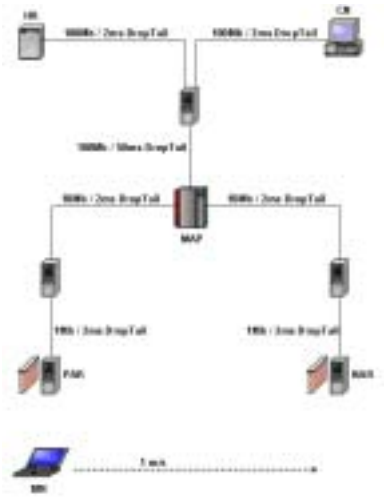

Figure 7 Network topology for simulations.

We evaluate the proposed scheme with network simulator ns-2 under the simulation network topology shown in Figure 7. The transmission performance of MN during handover period is what we want to know. There are one mobile node (MN), one corresponding node (CN), two access routers (PAR&NAR), one mobility anchor point (MAP) and one home agent (HA) in the simulation network. The communication range of all nodes with air interface is 50 m. The distance between PAR and NAR is 70 m and the overlap of communication range is about 30 m. The simulation starts at 0 second and ends at 80 second.

A TCP sender (CN) starts to send packets at 5 second until the end of the simulation and the MN begins to move from the PAR to the NAR at 10 second with moving speed 1 m/s and data rate 1 Mb/s. Also an UDP sender (CN) starts to send packets with rate 100 Kb/s at 5 second till the end of simulation. The packet size is set to 1K bytes. Authentication processing is 100ms as default. Each packet is given a sequence number. By checking the packet sequence numbers we can observe whether packet is received by the mobile node or it is lost. We compare the performance between the pre-authentication and formal authentication without pre-authentication.

The handover begins at about 40.46 second, so we show the result from 40 second to 45 second. As shown in Figure 8, the MN can not receive any packets from the TCP sender (CN) during the handover period. Packets are dropped because MN doesn't authenticate with target AR (AP) until it completes the authentication. The number of lost TCP packets increases slowly if we increase authentication processing time quickly. This result is due to TCP sliding window effect. The mobile node can't receive the packets dropped by Access Router if it doesn't authenticate with that AR. Therefore, the sender can't receive the ACKs from the receiver. The packets of offered window may be dropped by AR due to authentication mechanism. TCP sender (CN) will retransmit the first packet of offered window if the packets of usable window are sent and the TCP sender doesn't receive any ACKs from the receiver. Obviously the delay in receiving packets after L2 handoff varies depending on different authentication processing time. Also, this delay may interrupt the TCP connections between the sender (CN) and the receiver (MN).

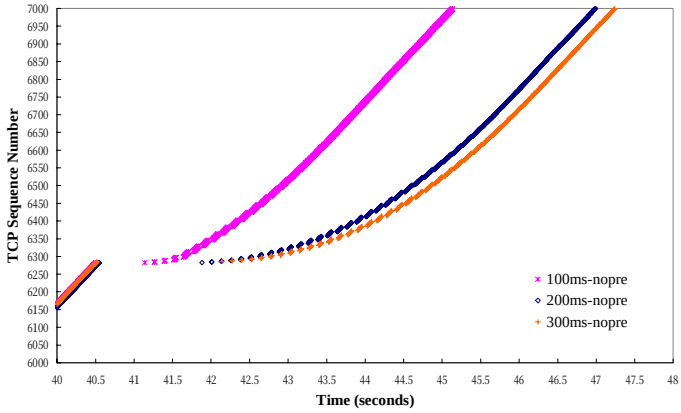

Figure 8 100ms-300ms authentication cases without pre-authentication

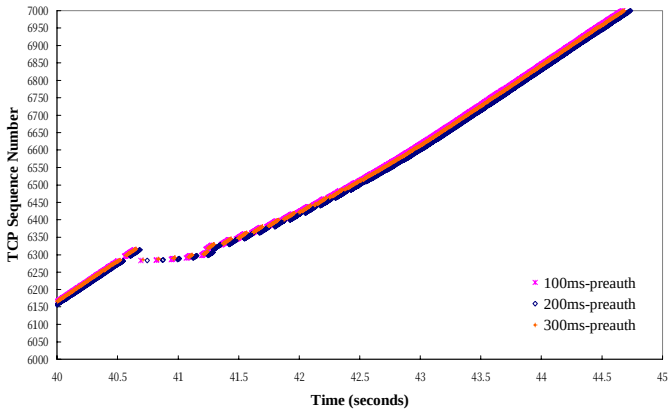

Figure 9 100ms-300ms authentication cases with pre-authentication

Figure 9 depicts the performance when pre-authentication scheme is performed. If the mobile node decides to handoff to new target domain, it will pre-authenticate with that target AR (AP) through fast handover protocol to reduce the handoff time and to receive packets again with minimum latency.

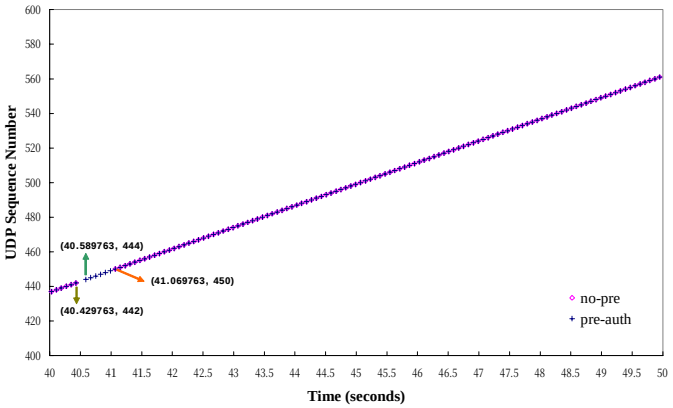

Figure 10 UDP with 100Kbps data rate

By observing the Figure 10 and Figure 11, we can find that the number of lost packets with pre-authentication is much lower than without pre-authentication. The packet loss rates with pre-authentication scheme are 8% and 13.6% for sending rate 100Kbps and 1Mbps respectively. For a multimedia streaming service, low packet loss rate is an important factor for quality of services.

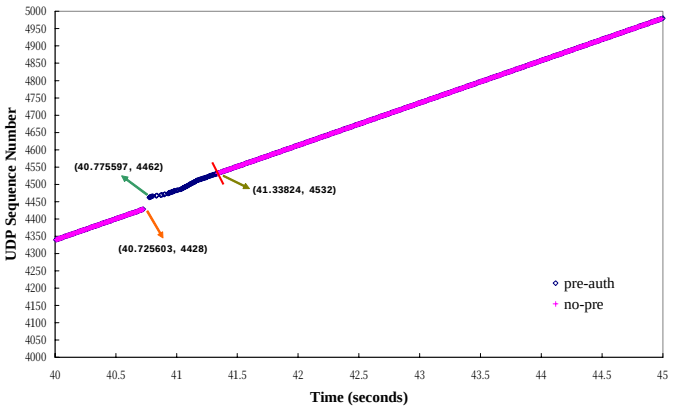

Figure 11 UDP with 1Mbps data rate

Sending rate	No. of packet drops		Packet loss rate	
100Kbps	8	2	32%(no-pre)	8%(pre)
1Mbps	104	34	41.6%(no-pre)	13.6%(pre)

Table 1 Packet drops versus Packet loss rate

Table 1 depicts the packet loss rate increases when sending rate raises. We can find that the packet loss rate increases if the authentication processing time increases, as shown in Table 2.

In short, two-stage authentication scheme features much lower packet loss rate and much shorter handover latency. The simulation results demonstrate the effectiveness of our proposed scheme.

Auth. processing time	Packet loss rate	
100ms	41.6% (no-pre)	13.6% (pre-auth)
300ms	100% (no-pre)	34.4% (pre-auth)

Table 2 Packet drops versus auth. processing time

五、結論與討論

The two-stage authentication scheme can enhance the performance of wireless handover if authentication mechanism is used. Different from the L3-FHR authentication scheme that authentication information is broadcasted by gateway to all L3-FHR ARs(APs), a MN just sends a copy of authentication information to the target ARs (APs) in two-stage authentication scheme. As a result, our proposed scheme can reduce the packet loss rate and authentication time. Our scheme can reduce the original IEEE 802.11 authentication process time because it pre-sends the identity of the MN to target AR(AP). We try to modify this scheme to co-work with IEEE 802.1x to reduce the authentication time and to provide a better authentication mechanism during handoff period in the future research.

六、參考文獻

[1] S. Pack et al., “Fast handoff scheme based on mobility prediction in public wireless LAN systems,” IEE Proceedings, Vol. 151, October 2004

[2] Nicolas et al., “Handover Management for Mobile Nodes in IPv6 Networks,” IEEE Communications Magazine, August 2002

[3] Rober Hsieh et al., “Performance analysis on Hierarchical Mobile IPv6 with Fast-handoff over End-to-End TCP,” Proceedings of GLOBECOM, Taipei, Taiwan 2002

[4] M.S. Bargh et al., “Fast Authentication Methods for Handovers between IEEE 802.11 Wireless LANs,” WMASH’ 04, October 1, 2004

[5] K. Malki et al., “Low Latency Handoffs in Mobile IPv4,” IETF Draft, draft-ietf-mobileip-lowlatency-handoffs-v4-04.txt, June 2002

[6] The Network Simulator - NS2, http://www.isi.edu/nsnam/ns