Mobile Intelligent Agent Technologies to Support Intelligent Handover Strategy

Chen-Han Lin and Jen-Shun Yang

Computer and Communications Research Laboratories, Industrial Technology Research Institute, Hsinchu, Taiwan, R.O.C.

Email: {chenhlin, jsyang}@itri.org.tw

Ko-Ching Wu

Department of Computer Science and Information Engineering, National Chiao Tung University, Hsinchu, Taiwan, R.O.C.

Email: wukc@csie.nctu.edu.tw

Abstract

We investigate the possible application of Mobile Intelligent Agent for early authentication prior to the handove. Seamless handover is required in VoIP mobility services in order to limit the period of the service disruption experienced by a MN when moving between different IP subnets. Our seamless handover method involves early deployment of multiple copies of the Mobile Intelligent Agents to predicative locations where the MS is about to move for early authentication. The implementation aspect of seamless handover in Mobile Agent based VoIP services is provided. In the performance analyses, a comparison in the handover delay is made between the standard Mobile IP mobility and our proposed method.

Keywords: VoIP mobility, corner effect, seamless handover, VPN, Mobile Agent, SIP, Mobile IP

I. Introduction

One of the most important factors in the success of VoIP mobility services seems to be the seamless handover that has made it possible to minimize the delays during the handover. The delays in the respect are the authentication and dynamic IP address allocation delays, which cause the packet loss. A Mobile Node (MN) sends multiple copies of the Mobile Agent (MA) to potential MN movement locations for pre-authentication. To eliminate the packet loss during handover, we employ the multi-homing concept that is the ability for a single endpoint to support multiple IP addresses. We rely on Virtual Private Network (VPN) connectivity method to reduce the delay of dynamic IP address allocation. Adding the improvements together will make the handovers in VoIP mobility services “seamless”.

The period from when the MN last receives data traffic via its old IP subnet to when it receives data from its new IP subnet is often referred to as the handover delay. Accordingly, the delay can be divided into four sub-delays, i.e. Layer 1/Layer 2 (L1/L2) radio link switching delay, L2 access re-authentication delay, IP layer binding delay and application layer authentication and registration delay. The sub-delays is described as follows.

Between the time a MN detaches from old link and attaches to new link, it's basically unreachable. The delay incurred to this exchange is referred to as the L1/L2 radio link switching delay. The delay is strictly hardware delay, which could be affected by the performance of network adapter and solved in the prior art of Intelligent Channel Scan mechanism [1]. The L2 access authentication, referred to as link layer (IEEE 802.1X [25]) authentication, occurs when the MN attempts authentication with a new AP. It may create a trust relation between the client and L2 access devices to ensure the cryptographic-protected WLAN access.

The IP layer binding delay is result from the allocation of dynamic IP address via DHCP followed by the routing path update to the new AP. Upon authentication success, a new IP address is assigned to the MN before the upper-layered handover could proceed. For the inter-AP handoff, Inter-Access Point Protocol (IAPP) is proposed in IEEE 802.11f [2]. The L2 re-authentication delay could be reduced during inter-AP roaming.

To reduce the connectivity delay and packet loss, G. Tsirtsis et al. proposed a fast handover scheme based on the Mobile IPv6 mechanisms [8]. A MN is assigned a new IP address even before it connects to its new AP. The process includes sending messages indicating handover to the MN, allowing it to form a new IP address, and negotiating the APs with this new IP address. A forwarding path from the previous AP to new AP is setup for the packets destined for MN’s previous IP address. The MN sends a “Fast” Mobile IPv6 Binding Update message to the previous AP only after receiving the forwarding indication.

There still remain many challenges in reducing the DHCP delay in proposed mechanisms such as SIP mobility [3] and Mobile IP [4], and application layer authentication and registration delay in SIP mobility [3]. We take advantage of VPN technology, where the MN is identified by its static private IP address regardless of its current point of attachment to the subnets, and allow the MN to use the same IP address during handover (in contrast to CoA in Mobile IP). When the mobile host hands off to any other AP, since the new AP receives session information in advance, further message exchanges are not needed. The relocated MN can obtain all information from the new AP and it is not necessary to send an “Access Request” request to the AAA server. Hence, the delay of re-authentication for the MN is reduced. On the Mobile IPv6 systems, the packets are forward from the old AP to the new AP, which could results in the reception delay and packet loss. Generally, since the AAA server is often located in a remote domain for more scalable service, the delay in the path from the AP to AAA server is a critical factor in the overall handover delay.

The rest of paper is organized as follows. Section 2 gives the background on current VoIP mobility methods

including MIP, SIP as well as the overview of major MA systems. Section 3 presents our solutions for solving the IP address allocation and authentication delays. Further details the appropriateness of MAs in wireless handover services. Section 4 discusses the performance of our proposed system. Section 5 concludes this paper.

II. Related Works

In this section, we describe the previous works related to mobility supporting for VoIP services. First, we present two major technologies, Mobile IP and SIP, for supporting mobility services in mobile environment. Second, detail the fast handover for Mobile IPv6. Third, present the multihoming and street corner effects. Last, briefly describe the overview of MIA technology.

A. Mobile IP

When a MN is away from its home, a Care-of Address (CoA) is temporarily assigned to the visiting MN, either by the Foreign Agent (FA), or by other means such as DHCP. After the allocation of new CoA, the MN then sends a Binding Update message to inform MIP agents to change the binding list of the MN to the new CoA. At the same time, HA updates the corresponding Binding Cache with new CoA in order to correctly forward packets destined to the MN.

A well-known problem in Mobile IP is triangular routing and call disruption. The triangular routing can be solved by the Route optimization mechanisms, where the binding updates are sent to inform the Corresponding Node (CN) about the actual location of the MN. The Call disruption caused by the CoA assignment and binding update completion delay could be solved by fast handover mechanisms [8].

B. SIP mobility

Wedlund and Schulzrinne proposed mobility support in the application layer protocol SIP where applicable, in order to support real-time communication in a more efficient way [5]. If the mobile node moves during an active session, first it obtains a new IP address from the DHCP server, and then sends a new session invitation to the corresponding node (CN). With this new invitation, it tells its new IP address so as to forward packets properly. As opposed to an MN using MIP (when the MN detect movements, it can obtain CoA from a FA), a MN using SIP-mobility always needs to acquire an IP address via DHCP, which can be a major part of the overall handover delay.

C. Fast handover for Mobile IPv6

This section is to further discuss the issues in handover we face. Let us assume that the MN migrates from the subnet of one AR to another. What problem are we going to face? What solution is currently available?

Initially an MN is attached to an AR (called old AR or Pervious AR: PAR) and moves into the range of another (called new AR: NAR). When it moves away from its PAR, the signal strength from the PAR will decrease. The MN must establish link connectivity with its NAR immediately before severe degradation of its PAR signal strength. Prior to attachment, it must somehow detect whether it has moved into the new access area. Once moved, it needs to configure new CoA. To form a new CoA, the MN requests the PAR to supply IP address, link-layer address as well as network prefix of the NAR's interface to which it is handing over to. Once CoA is configured, it must inform the HA and the CN of its new location by the means of Binding Update message. Before these tasks to be taken, the CN continues to transmit packets with the old CoA to PAR. From now on, if the MN is out of the range and no longer receives packets from its PAR, the packet loss occurs. For delay non-sensitive connection, a retransmission can be used to compensate for packet loss. But for delay sensitive connections, the retransmission delay may be intolerable. Thus, the fast handover for Mobile IPv6 has been proposed to solve the packet lose problem and to achieve the goal of smooth handover. The following section examines the Mobile IPv6 handover procedure in detail.

When an MN is about to move to another AR, it must send the **Routers Solicitation for Proxy** (RtSolPr) message to its PAR. In the **RtSolPr** message (*Router Solicitation for Proxy*), the MN must indicate the link layer address or the identifier of the attachment point to which it wants to move. The PAR will reply with a *Proxy Router Advertisement* message that contains a new CoA that the MN should use and the NAR prefix that should be used to form a new CoA. After that, the MN will send a Fast Binding Update (**FBU**) to its PAR to indicate its movement and that it wants its packets be forwarded to the NAR and further to him. At the same time, the PAR sends an ICMPv6 related **HI** message (*Handover Initiate*) to the NAR by indicating the old and the new CoA of the MN. If the NAR receives **HI** message (sent by PAR) without a new CoA, it will allocates a new **CoA** and sends it to the **PAR** by the means of *Handover Acknowledgement* (**HAck**) message. Otherwise, the **NAR** receives **HI** message with a new CoA, and it will determines if that new CoA is valid (or legal) and sends a validation indication in the *HAck* message. If the **HAck** message indicates that the new CoA is valid, the PAR will prepare to forward the packets to the MN with its new CoA. In the contrary case, if the **HAck** message indicates that the new CoA is invalid, the **HAck** has contained a valid new CoA allocated by NAR**.** On the reception of **HAck** message, the **PAR** must send *Fast Binding Acknowledgement* (**FBack**) to the MN by locally or by way of the NAR (by using the new CoA or by the address encapsulation in the NAR). On the **FBU** reception and the **FBack** sending, the PAR can start to forward the intended packets for the MN to the NAR with the MN's old CoA or with the MN's new CoA depending on the **HAck** message value. The NAR will cache these packets waiting for the MN handover to the **NAR.** When the

MN establishes link connectivity with the NAR, it must send a *Fast Neighbor Advertisement* (**FNA**) to initiate the flow of packets that may be waiting for it, or if it has not received confirmation in **FBack** message to use the new CoA. Once it is acceptable to use new CoA corresponding to the **FNA** message, NAR must enable the host route entry so that any unbuffered packet could be delivered. Finally, the MN must send *Binding Update* (**BU**) message to the HA and the CN through the NAR in order to register its new CoA. After the CN successfully process the **BU**, which involves the Return Routability procedure [], the MN can receive packets at new CoA. Handover completes.

Handover affects the network in various ways but it introduces two key problems: handover delay and packet loss. The above handover scheme is actually similar to the present GSM/GPRS handover. The common goals are to minimize the delay and packet loss at handover. To reduce handover delay, the MN registers with NAR through the PAR before leaving the old access area. To eliminate packet loss, the PAR uses the tunnel established between PAR and NAR to forward undelivered packets to NAR. The approach is considered essential for the delay-sensitive connections.

D. Link Layer Support of Multi-homing

Because Soft handover provides same data receiving from multiple APs, it allows MN's session to progress without interruption when a MN moves from one subnet to another. These can be done, if and only if (1.) MN is able to communicate simultaneously with multiple APs in the same time. (2.) The network can duplicate and correctly merge the IP flows from the CN to the MN through different APs. If the two conditions are verified, it is possible to eliminate packet loss and reduces end-to-end transmission delays, which provides a clear advantage to traffic requiring real time transmission.

Fast handover bi-casting, enables data duplication through old and new APs, but MN cannot receive more than one IP data flow at the same time. It enables data reception from multiples APs simultaneously at IP layer, which allows MN's session to progress without interruption when it moves from one AP to another. It requires MN to have two WLAN radio interfaces [9].

The multi-homing feature enables the MN to support seamless handover by simultaneous binding of two different addresses while staying the overlapping region. The packets are multicast to MN and MIP agents without need to tunnel packets to the NAR from the PAR as current present in Mobile IPv6 networks. The packet loss is reduced during the handover.

E. Street Corner Effect

Turning around a corner of a street can cause a sudden power-drop of 10-30 dB. This effect is called "Street Corner Effect". If a mobile station (MS) is assigned to a certain base station (BS), then the power-drop can cause a temporal loss of frames during the handover to the new BS. This mainly concerns fast moving MS's as used in cars. The effect can be mitigated by putting the target BS into the active list of serving base stations. To avoid an increased signalling traffic between the mobile and the active base stations, the decision errors have to be kept to a minimum. This can be partially achieved having a thorough knowledge of the radio wave behaviour during such power-drops. Thus, the objective of the project was to investigate the depth, duration and shape of a power-drop during a street corner turn-round in dependency of the assigned cell (Macro, Micro, Pico, etc.), the surrounding terrain and the MS speed.

Mobile Intelligent Agent technique is employed to reduce the application handover delay and packet loss ratio. The Mobile Intelligent Agent is traveled along the electric field to the neighboring subnets. The dispatch of Mobile Agents must occur enough in advance so that it is possible for the Mobile Agents to authenticate with the new access router. First, the MN measures the power and discards all unknown patterns to exclude complete failures in the decision making. Second, known pattern are followed to distinguish between a temporarily shadowed mobile and a real power drop occurrence. Once the power drop pattern falls below a chosen threshold, the handover is initiated. On the one hand, the threshold is chosen to be higher than the dynamic thresholds for the existing soft-handover hysteresis algorithms. This yields the required gain in handover processing time. And on the other hand, the threshold has to be sufficiently low to minimize falsely initiated handover. The actual value of the threshold, however, is quite crucial in the performance of the system and will vary from location to location.

F. The Mobile (Intelligent) Agent Technology

In recent years the mobile intelligent agent technology has been the focus of much speculation. The MA is software component include data and executable code, which can be transferred from network element to another while carrying on its status of execution. The MA is a quite alluring technology which can walk everywhere in Internet to search for application relative information [14]. It can find us a great deal of goods and services, and interact with other MA within the same network or remain bound to a particular host. Also, as shown in [12], in certain cases, the MA technology can diminish network traffic compared to traditional client-server model and maintain load balancing, thus improve network performance especially in mobile environment. So we take advantage of MA technology to assist the SIM-based pre-authentication. The MA technology not only reduces control packets to process the SIM-based authentication but also pre-create a VPN tunnel at the new location of attachment for secured packet transmissions.

The future mobile communications are becoming personalization and customization. Thus we expect that the future mobile services can enable the nomadic users using multi-homed device to access any tier of heterogeneous

wireless networks (e.g., WLAN and 3G cellular network) anytime and anywhere with the information that agrees with the manners recorded in each user's profiles. However, this requires a very sophisticated and appropriate infrastructure to carry out personalization such as those foreseen in the Virtual Home Environment (VHE) [10] and the Personal Service Environment (PSE) [11]. Such a mobile environment should enable a seamless integration of complex and distributed heterogeneous wireless and fixed networks. One of the seamless integration is obviously the combination of WLAN and 3G architectures, which is desirable in order to deliver ultimately personalized end-to-end mobile services. This architecture would be met by MA technology maturely. So recently, there was a work on the MA-based advanced service architecture for wireless Internet telephony [15].

We have emphasized the advantages of a MA-based technology for brokerage of personalized movable devices. In this work, the term MA is referred to any entity that process a particular task on behalf of one of the players (MNs) mentioned above. In order to conceive and build agent system platforms (i.e. agent development environments), the players with capabilities are required to create and execute agents therein. Because MIAs are deemed so popular, there has been an explosion of platforms being created for developing agent and multi-agent systems. Following this development, several standardization efforts are underway, namely by FIPA [16] and OMG [17]. Some well-known MA systems [13] are: MOLE, Telescript, Aglets Workbench, ffMAIN, and D'Agents. Despite the fact that these system were built to serve the same purpose, they have many differences in terms of terminology, concepts, and architecture. Some of these systems were developed in academic environments and others were developed by the industry.

III. Mobile (Intelligent) Agents to support seamless VoIP services over Mobile VPN

The MA-based pre-authentication system includes the seamless handover architecture for mobile VPN and the seamless handover mechanism, which employs the MA technologies to facilitate early authentication and registration of MN over a new AP. The delay can be minimized if the MAs are dispatched to the new IP subnet as soon as possible. To do so, we utilize link layer (layer 2 or L2) triggering events to improve handover. IEEE 802.21 working group proposed the L2 triggering [23]. The MAs will be dispatched (or forked), whenever there is such triggering event in prior to an occurrence of the actual handover.

Both IP layer binding delay and application layer authentication and registration delay are major parts of the overall handover delay. The delay of IP address renewal (> 2s) has significant effect on the overall handover performance. The application layer authentication and registration delay is harder to reduce than the DHCP delay and cannot be ignored due to security consideration.

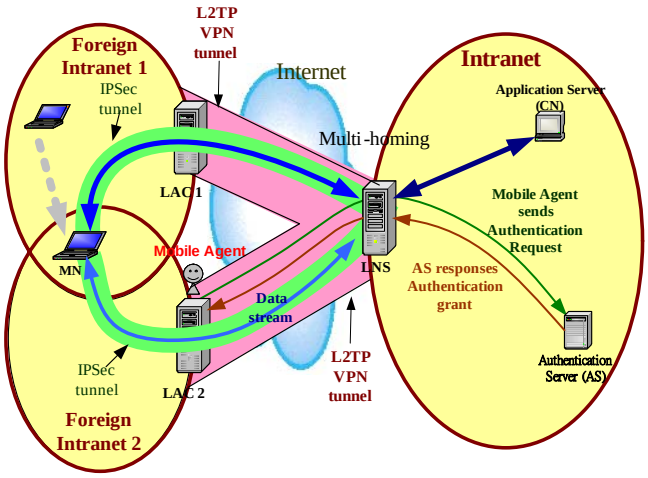

Fig. 1 Seamless Handover Architecture for Mobile VPN

To overcome these drawbacks, we propose the seamless handover architecture for the mobile VPN users (Fig. 1). Layer 2 Tunneling Protocol (L2TP) VPN tunnels are constructed between the L2TP Network Server (LNS) and all L2TP Access Concentrators (LACs). Service and authentication requests and data packets are protected under IPSec tunnels while transmitted between the MN and LNS. They are further encapsulated into L2TP VPN tunnels during transmission between the LNS and LAC. The LNS function as a service proxy to forward the service requests from the MN to the application server. To minimize the DHCP delay, IP binding update delay, and application layer authentication delay, we employ the following three techniques.

- VPN with private static IP address
- Multi-homing
- Mobile Agent

It is desirable for the MN to be able to keep the same IP address while roaming. L2TP VPN can be implemented as an Intranet and have the static private IP addresses assigned to its private MNs regardless of their location. The MN can remain connected to its home network over the L2TP VPN tunnels while roaming among different foreign Intranets (i.e., IP subnets). For the purpose, we can ignore the delay of IP address renewal (i.e., CoA delay in Mobile IP and DHCP delay in SIP).

The fast handover for Mobile IPv6 [8] tries to minimize the period of service disruption by the packet tunneling mechanisms while performing network layer handover. In contrast to the fast handover for Mobile IPv6, the multi-homing concept is used to minimize the disruption time and packet loss ratio. Traffic for the MN bi-casts or multicasts to its current location and to one or more locations where the MN is expected to move to shortly. The ambiguity of the data traffic timing for the MN to its new point of attachment following the fast handover can be

avoided, which allows decoupling of the L2/L3 handoffs. Although bi-casting or multi-casting requires more network bandwidth, it eliminates the service disruption period currently present during handoffs in Mobile IPv6 networks due to end-to-end transmission delay caused by the triangle routing.

Note that many WLAN providers will block all outbound traffic from the MNs until the authentication and authorization are completed. They adopt the EAP-SIM based authentication [24] mechanism to take advantage of high security and needless user's intervention. The MA, carrying the user's profile and SIM info, executes the EAP-SIM based authentication over the L2TP VPN tunnels prior to the L2 handover.

In Fig. 2, we illustrate the handover cycle, defined as a sequence of phases in a single handover procedure starting with the handover request from the MN, and ending with old handover path is completely removed.

- **Phase 1 – Prior to the handover**

Initially an MN is attached to one LAC and moves into the range of another. In order to restrict the access to the VPN and the application server (i.e., CN), the MN initiates the EAP-SIM based authentication to the Authentication Server (AS) prior to the registration of an application, whereof the EAP-SIM based authentication is slightly revised from original version due to adopt to the application layer. Here, the LNS play the role that is originally responsible by the AP with IEEE 802.1X [25] capability in the EAP-SIM based authentication. In Fig. 2, we abstract the signals of EAP-SIM based authentication in two messages: **Authentication Request** and **Authentication Response**. Once authenticated, the MN can register to the application server and then establish connection with the CN before packet transmission. Thereafter, LNS can intercept the packets from CN and tunnels them to the LAC where the MN is associated, or vice versa. An LAC is the access router of a subnet and responsibility to tunnel the packets from/to the LNS. Our deployment of LAC is in accordance with the assumptions that no more than two individual LACs are located in the same Foreign Intranet and the APs in a Foreign Intranet are all assigned an identical Extended Service Set Identification (ESSID). Hence, an MN located within a Foreign Intranet can recognize the neighboring Foreign Intranet by the ESSID value carrying in the link-level beacons and to determine the numbers of neighboring LACs. Periodically, each AP sends out a link-level beacon containing ESSID that can let MNs to measure the signal strength and to recognize the Foreign Intranets. After completing the EAP-SIM based authentication, the LNS who also plays the service proxy in the VPN home network will send an Access-Accept message to the application service (i.e., CN) in order to notify the application service about the authentication successful. This action can enable the following legal service registration and the session setup procedures.

- **Phase 2 – Beginning of the handover**

When the radio signal strength of the current AP starts weakening, the MN tries to look for a better AP to re-associate with, triggering a handover procedure. If the radio-signal strength in the current Foreign Intranet is lower than a certain threshold, it finds out which neighboring Foreign Intranets with different ESSID have the radio signal strength higher than the threshold and dispatches MAs to the corresponding LACs of the Foreign Intranets. Here, the LACs is been carefully chosen in accordance with if some strategies, for example the choice can be done by the mobility predictions, but which are beyond the discussion of this paper. It should be noted that the number of the LACs been dispatched MA have to inform the LNS, because the LNS will multicast the data packets to the LACs, and then the packets will be further forwarded toward the radio links during the period when the MN ready to handover into one of the LACs. The multicast among possible LACs could reduce the disruption time and also the packet loss. After arrived at each LAC, the MA authenticate with AS on behalf of the MN while waiting for it to arrive, whereof the LAC forward the authentication information to the LNS via the tunnels. Since duplicated authentication information are forwarded to the LNS, the LNS merges these information and forwards them to AS. Once authenticated, AS notifies LNS about the granted access rights of the MA to use the tunnel. The LNS then forwards the notification to the LAC where the MA is associated. The associated IP address of the LACs is added to the binding list in LNS. After the authentication, LNS maintains multiple communication paths between the MN and its CN. The multicast traffic the mobile node delivers to its CN or vise versa is sent via the LNS-LACs pairs VPN tunnels, which are based on multi-homing conception.

- **Phase 3 – Ending of the handover**

Once the MN moves out the range of its original LAC and into that of a pre-authenticated LAC, a secure communication is setup with its MA. The MN receives the secured report from its MA including granted access rights of its MA to use the tunnel. After authentication, the MN gets full access to use the tunnel. It starts receiving the undelivered packets on the tunnel as soon as the connection to its LAC is established. After attached to the new LAC, the mobile node must inform the LNS of its new location by the means of Location Update message which results in the unicast traffic. Finally, if there are no packets transmitted within a specific time period, the connection to the old LAC via the old routing path is closed, and the MAs in the other neighboring LACs are removed by the notification of L2TP Hello message sending from LNS.

IV. Performance analysis of seamless handover

In the performance analyses, a comparison is made between the handover delay of the original Mobile IP system and that of the proposed system above (Fig. 3). The original Mobile-IP system is shown in the left part of the Fig. 3. The handover procedure begins when the MN initiates its L2 handover or the signal strength in the current subnet is lower than a certain threshold. The L2 handover lasts approximately 100ms. The handover procedure continues when the MN acquires an IP address from a DHCP server. The delay for the dynamic IP address allocation approximates 2s. The handover procedure continues with L3 handover. The delay for L3 handover is around 542ms. The handover procedure ends with the service authentication and registration. The delay for the service authentication and registration is around 3s. The overall delay is around 5.6s.

The proposed Mobile-Agent based pre-authentication system is shown in the right part the Figure 3. Our proposed system solves most of handover incidents that cause delay. First, we proposed a solution for the reduction of the dynamic IP address allocation delays via the VPN connectivity. Then, we proposed the MA pre-authentication mechanisms to solve the application layer authentication and registration delay. Ideally the application layer authentication and registration are finished in advance, so the changing of the subnet at a later point of time can be carried out with minimum delay and no uncertainty about resource availability. The MN dispatches the MAs to the neighboring Foreign Intranets when it is still delivering/receiving the packets over the old Foreign Intranet. So the initial timeline for our proposed system is moved ahead of that of the Mobile-IP system. Besides, we employ the multi-homing concepts to minimize the packet loss during the handover. By configuring the VPN tunnel to provide static IP address allocation and performing MA pre-authentication during the L2 handover, the overall delay was greatly reduced from 5.6s to about 100 ms.

The delay analyses are described as below. Here, each presented delay is the average value from the experimental results referred from [26].

L2	L2 handover delay	IPA	DHCP (IP address) delay
L3	L3 handover delay	DIS	DHCP Discovering delay
SA	Service Authentication	OFR	DHCP Offering delay
PR	Probe delay	REQ	DHCP Request delay
AU	Authentication delay	ACK	DHCP ACK delay
RA	Re-association delay	AAD	Average Agent discovery
BU	Binding update delay	REP	Reply message delay

Handover delay = ***L2*** + ***IPA*** + ***L3*** + ***SA***,
where ***L2*** = PR + AU + RA ≅ 100 ms,
IPA = DIS + OFR + REQ + ACK ≅ 2s,
L3 = AAD + ***BU***+ ***REP*** ≅ 542ms.

However, the delays in service authentication and registration could be varied by two factors, i.e. the distance between a MN and AS, and the retrieval time of user profile from HLR/VLR. The sum of these delays would average 3000ms (or 3s).

DHCP delay is explained as below. As the first-time register of the DHCP client to the server, the client has four steps as described in Fig. 4 to complete the register. The first step is looking for the DHCP server. The client would send a DHCPDISCOVER packet to the network with 0.0.0.0 as its source address and 255.255.255.255 as its destination address. The default DHCPDISCOVER waiting time of Windows is set to be 1 second, in other words, if the client didn't receive the response, it would send the second time of DHCPDISCOVER, and the next waiting time would be set to be 9 seconds (and 13, 16 seconds as follow). The second step is for DHCP server to offer a rent of IP address. When the DHCP server has listened to the DHCPDISCOVER broadcast, it would select an unused IP address with other TCP/IP setting to be included in the DHCPOFFER response to the client. The third step is for DHCP client to accept the rent of IP address. If client received multiple responses form different servers, it would only choose one to reply DHCPOFFER (usually the first arrived). Then client would broadcast a DHCPREQUEST to inform all servers what it chose. The last step is to confirm the lease. After the server has received DHCPREQUEST, it would send a DHCPACK to the client, and finish the procedures.

Beside, the Layer 3 handover delay is caused by the process of standard Mobile IP handover. The standard mobile IP handover implementation initiates a network-layer handover only upon reception of an agent (the fixed MIP agent) advertisement in the agent discovery procedure, which takes 500ms for average (the half of advertisement duration), and followed by the DHCP procedure. Subsequent mobile IP processing may take around 35ms~50ms, which is varying depending on the network delays. Hence, the Layer 3 handover averages 542ms.

By comparing to the original Mobile-IP, our proposed Mobile-Agent Pre-authentication system remains only the L2 handover delay. Even if the multi-homing is not supported due to the fact that the multi-homing causes more bandwidth utilization, it may induce the average handover delay to extend to 642ms.

V. Conclusions

We investigate the delay of different layers of network protocol stack (e.g., link layer, network layer, transport layer, and application layer) and develop an efficient method to achieve seamless handover. We propose the architecture supporting the VoIP seamless handover to eliminate connection interruption during inter-AP roaming. Based on the mobile agent and multi-homing concepts, we could reduce the handover delay down to L2 radio link switching delay and packet loss ratio in addition to the fast handover for MIPv6 in the IETF draft. Although the MA-based pre-

authentication system requires more networks bandwidth, it only generates traffic when the MN wants exclusive access to its MA to renew the connection with foreign subnet. However, it eliminates the service disruption period currently present during handoffs in Mobile IPv6 networks due to end-to-end packet transmission delay caused by triangle routing.

VI. References

[1] Kyoungnam Kwon, Chaewoo Lee, "A fast handoff algorithm using intelligent channel scan for IEEE 802.11 WLANs," The 6th International Conference on Advanced Communication Technology, 2004, Volume: 1, Pages:46-50

[2] IEEE 802.11f/D3, "Recommended Practice for Multi-Vendor AP Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation," January 2002

[3] J. Rosenberg et al., "SIP: Session Initiation Protocol, RFC 3261," Internet Eng. Task Force, June 2002.

[4] C.E. Perkins, "IP mobility support," RFC 2002, IETF, October 1996.

[5] E. Wedlund and H. Schulzrinne, "Mobility support using SIP," Second ACM/IEEE International Conference on Wireless and Mobile Multimedia (WoWMoM'99), (Seattle, Washington), August 1999.

[6] Schulzrinne and E. Wedlund, "Application-layer mobility using SIP," ACM Mobile Computing and Communications Review, Vol.4, No.3, July 2000.

[7] D. Johnson, C. Perkins, "Mobility support in IPv6", Internet Engineering Task Force draft-ietfmobileip-ipv6-13.txt, November 2000.

[8] G. Tsirtsis, A. Yegin, C. Perkins, G. Dommety, K. El-Malki, M. Khalil, "Fast Handovers for Mobile IPv6", Internet Engineering Task Force draft-ietf-mobileip-fast-mipv6-00.txt, February 2001.

[9] ANSI/IEEE Std 802.11, "Wireless LAN Medium Access Control (MAC) and Physical layer", 1999 Edition.

[10] 3G Technical Specification 22.121, "The Virtual Home Environment, 3rd generation partnership project, Technical specification group services and system aspects," http://www.3gpp.org/

[11] A Mingkhwan, M. Merabti and B. Askwith, "IPMSA: integrated personal mobility services architecture" IEEE International Conference on Communications, ICC2002, May 2002.

[12] D. Chess et al. "Mobile Agents: Are They a Good Idea?," IBM Research Report RC (88465), 1994.

[13] M.K. Perdikas et al., "Mobile Agents Standards and Available Platforms," Computer Networks, vol.31, no.19, pp.1999-2016, Aug. 1999.

[14] A. Karmouch and V.A. Pham, "Mobile Software Agents: An Overview," IEEE Comm. Magazine, vol.36, no.7, Jul. 1998.

[15] B. Emako et al. "A mobile agent-based advanced service architecture for wireless Internet telephony: design, implementation, and evaluation," IEEE Transactions on Computers, Vol. 52, No. 6, Jun. 2003.

[16] FIPA, The Foundation for Intelligent Physical Agents, http://www.fipa.org/.

[17] OMG, Object Management Group, http://www.omg.org/.

[18] T. Gschwind, M. Feridun, and S. Pleisch, "ADK: Building Mobile Agents for Network and System Management from Reusable Components," ASA/MA'99, pp13-21, IEEE Computer Society, 1999.

[19] D. Dasgupta, and H. Brian, "Mobile Security Agents for Network Traffic Analysis," Proceedings of DARPA Information Survivability Conference and Exposition II (DISCEX-II), IEEE Computer Society Press, 2001.

[20] G. Cabri, L. Leonardi, and F. Zambonelli, "Agents for Information Retrieval: Issues of Mobility and Coordination," Journal of Systems Architecture, p1419-1433, 46, 2000.

[21] T. Tripathi, T. Ahmed, and N. Karnik, "Experiences and Future Challenges in Mobile Agent Programming," Microproc. Microsyst. P121-129, 25, 2, Apr. 2001.

[22] G. Huston "Architectural Approaches to Multi-Homing for IPv6," Internet-Draft: draft-ietf-multi6-architecture-00.txt, Jul. 2004.

[23] IEEE Std 802.21 Developing Group, http://www.ieee802.org/21/.

[24] Haverinen, H., Salowey, J.," EAP SIM Authentication" draft-haverinen-pppext-eap-sim-12.txt, October 2003.

[25] ANSI/IEEE Std 802.1X, "Local and metropolitan area networks—Port-based Network Access Control," 2001.

[26] Srikant Sharma, Ningning Zhu, and Tzi-cker Chiueh, "Low-Latency Mobile IP Handoff for Infrastructure-Mode Wireless LANs," IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 22, NO. 4, May 2004.

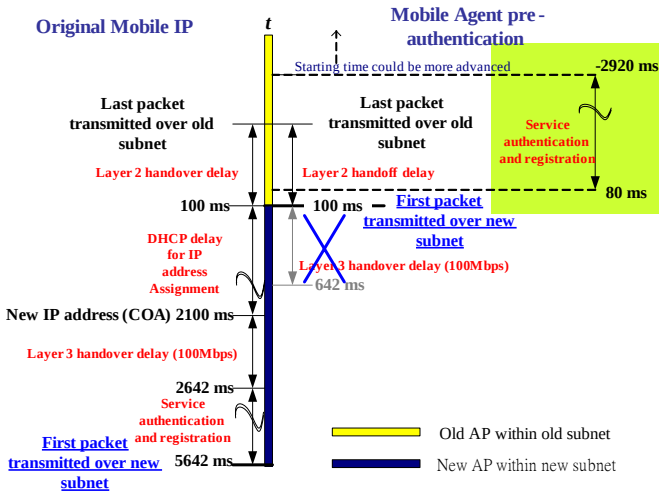

Fig. 3 Performance Comparison between the original Mobile IP system and the proposed Mobile Agent based Pre-authentication system

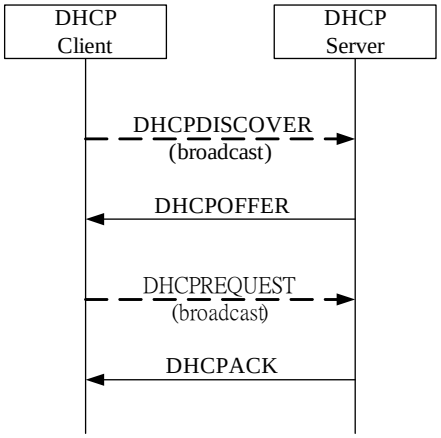

Fig. 4 DHCP Signaling

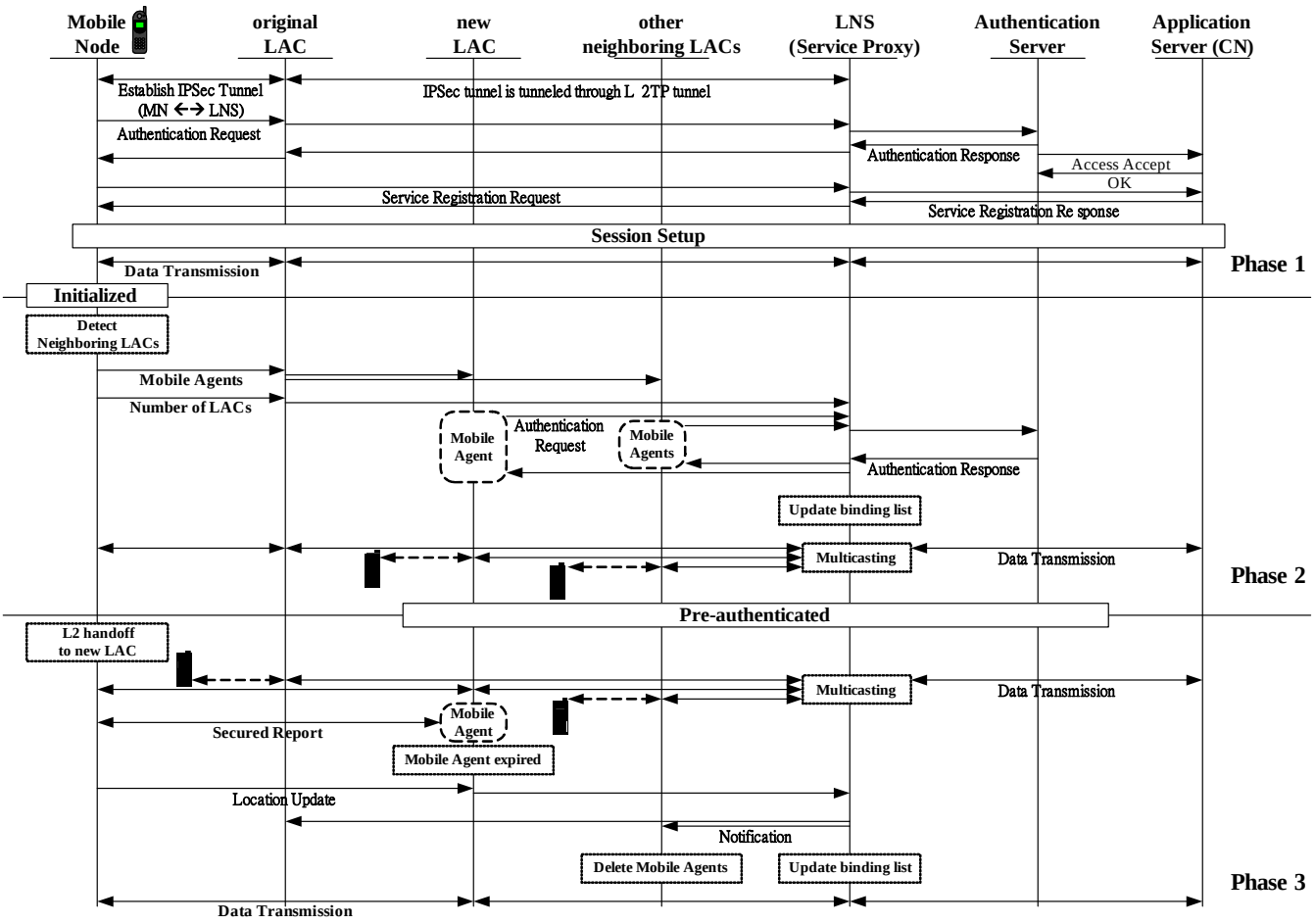

Fig. 2 message flow of whole handover procedure