

# MPA assisted Optimized Proactive Handoff Scheme

Ashutosh Dutta, Tao Zhang, Telcordia Technologies, NJ  
Yoshihiro Ohba, Kenichi Taniuchi, Toshiba America Research Inc., NJ  
Henning Schulzrinne, Computer Science Department, Columbia University, NY

## Abstract

In order to support session-based real-time communication in a highly mobile environment it is desirable to limit end-to-end delay, jitter and packet loss at a certain threshold level. This paper describes a framework of Media-independent Pre-Authentication (MPA), a new handover optimization mechanism that has a potential to address issues on existing mobility management protocols and mobility optimization mechanisms to achieve these values. MPA is a mobile-assisted, secure handover optimization scheme that works over any link-layer and with any mobility management protocol. This paper also presents an initial implementation of MPA and performance results to show how existing protocols could be leveraged to realize the functionalities of MPA and provide the desired results.

## 1. Introduction

As wireless technologies including cellular and wireless LAN become prevalent, supporting terminal mobility across different types of access networks, such as from a wireless LAN to CDMA or to GPRS is considered as a clear challenge. On the other hand, supporting terminal handovers between access networks of the same type is still more challenging, especially when the handovers are across IP subnets or administrative domains. To address those challenges, it is important to provide terminal mobility that is agnostic to link-layer technologies in an optimized and secure fashion without incurring unreasonable complexity. In this paper we discuss terminal mobility mechanism that provides seamless handovers with low-latency and low-loss. There are several mobility management protocols at different layers. Mobile IP [1] and Mobile IPv6 [2] are mobility management protocols that operate at network-layer. There are several ongoing activities in the IETF to define mobility management protocols at layers higher than network layer. For example, MOBIKE (IKEv2 Mobility and Multi-homing) [3] is an extension to IKEv2 that provides the ability to deal with a change

of an IP address of an IKEv2 end-point. HIP (the Host Identity Protocol) [4] defines a new protocol layer between network layer and transport layer to provide terminal mobility in a way that is transparent to both network layer and transport layer. Also, SIP-Mobility is an extension to SIP to maintain the mobility binding of a SIP user agent [5]. In order to provide desirable quality of service for interactive VoIP and streaming traffic, one needs to limit the value of end-to-end delay, jitter and packet loss to a certain threshold level. End-to-end delay is more of an issue for an interactive voice communication than the streaming traffic. ITU-T and ITU-E standards define the acceptable values for these parameters. For example for one-way delay, ITU-T G.114 recommends 150 ms as the upper limit for most of the applications, and 400 ms as generally unacceptable delay. One way delay tolerance for video conferencing is in the range of 200 to 300 ms. Also if an out-of-order packet is received after a certain threshold it is considered lost. Similarly a normal voice conversation can tolerate up to 2% packet loss.

While mobility management protocols maintain mobility bindings, using them solely in their current form is not sufficient to provide seamless handovers. An additional optimization mechanism is needed to help prevent the loss of transient data while updating the mobility binding so as to achieve seamless handovers. Such a mechanism is referred to as a mobility optimization mechanism. For example, there are existing mobility optimization mechanisms [6], [7] available to reduce the handoff for IPv4 and IPv6 networks respectively. There are some problems associated with the existing mobility management optimization techniques and there are some basic requirements that need to be fulfilled. 1) Existing mobility optimization mechanisms are tightly coupled with specific mobility management protocols. For example, it is not possible to use mobility optimization mechanisms designed for Mobile IPv4 or Mobile IPv6 to be used for MOBIKE. Thus a single, unified mobility optimization mechanism that works with any

mobility management protocol is strongly desired. II) Second, there is no existing mobility optimization mechanism that easily supports handovers across administrative domains without assuming a pre-established security association between administrative domains. A mobility optimization mechanism should work across administrative domains in a secure manner only based on a trust relationship between a mobile node and each administrative domain. III) A mobility optimization mechanism needs to support not only multi-interface terminals where multiple simultaneous connectivity through multiple interfaces can be expected, but also single-interface terminals moving between homogeneous access networks.

This paper describes a framework of Media-independent Pre Authentication (MPA), a new handover optimization mechanism that has a potential to address all those issues. MPA is a mobile-assisted, secure handover optimization scheme that works over any link-layer and with any mobility management protocol including Mobile IPv4, Mobile IPv6, MOBIKE, HIP, SIP mobility, etc. In MPA, the notion of IEEE 802.11i pre-authentication is extended to work at higher layer, with additional mechanisms to perform early acquisition of IP address from a network where the mobile terminal may move as well as proactive handover to the network while the mobile terminal is still attached to the current network.

Rest of the paper is organized as follows. We describe the related work in Section 2. Section 3 describes the MPA framework and its associated functional components. Some of the important issues and techniques that affect the mobility optimization are described in Section 4. Section 5 describes the results of implementation and compares it with Non-MPA-based architecture. Finally we conclude our paper in Section 6.

## 2. Related Work

While basic mobility management protocols such as Mobile IP [1], Mobile IPv6 [2], SIP-Mobility [5] offer solution to provide continuity to TCP and RTP traffic, these are not optimized to reduce the handover latency in its current form during mobile's frequent movement between subnets and domains. In general, these mobility management protocols suffer from handover delays incurred at several layers such as layer 2, layer 3 and application layer for updating the mobile's mobility binding. Mobility optimization mechanisms [6] and [7] are defined for Mobile IPv4 and Mobile

IPv6, respectively, by allowing neighboring access routers to communicate to carry information on mobile terminals. These provide fast-handover techniques that utilize mobility information made available by the link layer triggers. The CARD (Candidate Access Router Discovery Mechanism) protocol [8] is designed to discover neighboring access routers and is considered as helper protocol for mobile assisted handoff. There are few micro-mobility management schemes [9], [10], and intra-domain mobility management schemes such as [11], [12] that provide fast-handover by limiting the signaling updates within a domain. Yokota et al. [13] proposes joint use of access point and dedicated MAC bridge to provide fast-handover without altering MIPv4 specification. Shin et al [14] proposes a scheme that reduces the delay due to MAC layer handoff by providing a cache-based algorithm. [15] provides an optimized handover scheme for SIP-based mobility management, where the transient traffic is forwarded from the old subnet to the new one by using an application layer forwarding scheme. [16] provides a fast handover scheme for a single interface case that uses mobile initiated tunneling between the old foreign agent and new foreign agent. Some of the mobility management schemes use dual interfaces thus providing make-before-break scenario [17]. In a make-before-break situation communication usually continues with one interface, when the secondary interface is in the process of getting connected. The IEEE 802.21 working group is discussing these scenarios in details. Providing fast-handover using a single interface needs more careful design techniques than for a client with multiple interfaces.

The proposed MPA scheme described in this document is not limited to Mobile IP type mobility protocol only and in addition this scheme takes care of movement between domains, performs pre-authentication in addition to proactive handover and works for both single interface and multiple interfaces.

## 3. MPA Framework

Media-independent Pre Authentication (MPA) is a mobile-assisted, secure handover optimization scheme that works over any link-layer and with any mobility management protocol. With MPA, a mobile node is not only able to securely obtain an IP address and other configuration parameters from a candidate target network, but also able to send and receive IP packets using the obtained IP address and other configuration parameters, before it attaches to the candidate target network when one of the candidate target networks

becomes the next network the mobile moves to. This makes it possible for the mobile node to complete the binding update of any mobility management protocol and use the new care-of address before performing a handover at link-layer.

This functionality is provided by allowing a mobile node, which has a connectivity to the current network but is not yet attached to a candidate target network with the following set of procedures

- (i) Establish a security association with the candidate target network to secure the subsequent protocol executions,
- (ii) Securely execute a configuration protocol to obtain an IP address and other configuration parameters from the candidate target network as well as a tunnel management protocol to establish a bidirectional tunnel between the mobile node and an access router of the candidate target network,
- (iii) Send and receive IP packets, including signaling messages for binding update of a mobility management protocol and data packets transmitted after completion of binding update, over the tunnel using the obtained IP address as the tunnel inner address, and
- (iv) Finally delete or disable the tunnel immediately before attaching to the candidate target network when it becomes the target network and then re-assigning the inner address of the deleted or disabled tunnel to its physical interface immediately after the mobile node is attached to the target network through the interface.

In certain circumstances the tunnel may be deleted or disabled immediately after it is attached to the target network.

Especially, the third procedure makes it possible for the mobile to complete higher-layer handover before starting link-layer handover. This means that the mobile is able to send and receive data packets transmitted after completion of binding update over the tunnel, while it is still able to send and receive data packets transmitted before completion of binding update outside the tunnel.

In the above four basic procedures of MPA, the first procedure is referred to as "pre-authentication", the second procedure is referred to as "pre-configuration", the combination of the third and fourth procedures are referred to as "secure proactive handover". The

security association established through pre-authentication is referred to as an "MPA-SA". The tunnel established through pre-configuration is referred to as a "proactive handover tunnel".

### 3.1. MPA Functional Elements

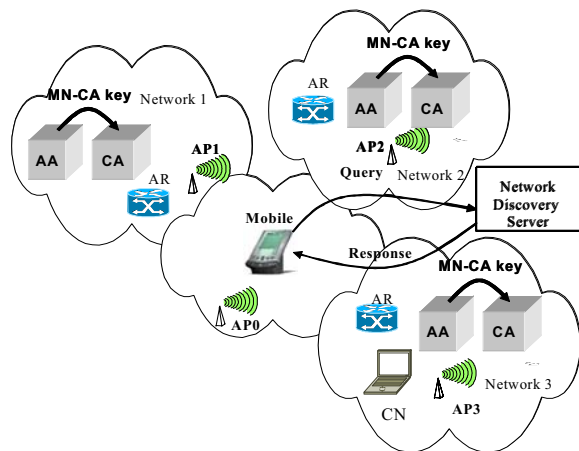
In the MPA framework, the following functional elements are expected to reside in each candidate target network to communicate with a mobile node: Authentication Agent (AA), Configuration Agent (CA) and Access Router (AR). Some or all of those elements can be placed in a single network device or in separate network devices.

An authentication agent (AA) is responsible for pre-authentication. An authentication protocol is executed between the mobile node and the authentication agent to establish an MPA-SA. The authentication protocol must be able to derive a key between the mobile node and the authentication agent, should be able to provide mutual authentication. The authentication protocol should be able to interact with AAA protocol such as RADIUS and Diameter to carry authentication credentials to an appropriate authentication server in the AAA infrastructure. The derived key is used for further deriving keys used for protecting message exchanges used for pre-configuration and secure proactive handover. Other keys that are used for bootstrapping link-layer and/or network-layer ciphers MAY also be derived from the MPA-SA.

A configuration agent (CA) is responsible for one part of pre-configuration, namely securely executing a configuration protocol that enables to deliver an IP address securely and other configuration parameters to the mobile node. The signaling messages of the configuration protocol must be protected using a key derived from the key corresponding to the MPA-SA.

An access router (AR) is a router that is responsible for the other part of pre-configuration, i.e., securely executing a tunnel management protocol to establish a proactive handover tunnel to the mobile node, and secure proactive handover using the proactive handover tunnel. The signaling messages of the configuration protocol must be protected using a key derived from the key corresponding to the MPA-SA. IP packets transmitted over the proactive handover tunnel should be protected using a key derived from the key corresponding to the MPA-SA. Figure 1 shows an example of network discovery aided MPA scheme

where a mobile discovers the details of neighboring network elements and proactively communicates with them to prepare for the handover to the target network. Network 1, Network 2 and Network 3 are possible target networks. Following describes the steps involved in providing the proactive handover. Assume that the mobile node is already connected to a point of attachment, say oPoA (old point of attachment), and has been assigned a care-of address, say oCoA (old care-of address).



**Figure 1: Network Discovery assisted MPA Framework**

**Step 1 (pre-authentication phase):** The mobile node finds a candidate target network through some discovery process and obtains the IP addresses of an authentication agent, a configuration agent and an access router in the candidate target network by some means. The mobile node performs pre-authentication with the authentication agent. If the pre-authentication is successful, an MPA-SA is created between the mobile node and the authentication agent. Two keys are derived from the MPA-SA, namely an MN-CA key and an MN-AR key, that are used to protect subsequent signaling messages of a configuration protocol and a tunnel management protocol, respectively. The MN-CA key and the MN-AR key are then securely delivered to the configuration agent and the access router, respectively.

**Step 2 (pre-configuration phase):** The mobile node realizes that its point of attachment is likely to change from oPoA to a new one, say nPoA (new point of attachment). It then performs pre-configuration, with the configuration agent using the configuration protocol to obtain an IP address, say nCoA (new care-of address), and other configuration parameters from the candidate target network, and with the access

router using the tunnel management protocol to establish a proactive handover tunnel. In the tunnel management protocol, the mobile node registers oCoA and nCoA as the tunnel outer address and the tunnel inner address, respectively. The signaling messages of the pre-configuration protocol are protected using the MN-CA key and the MN-AR key. When the configuration and the access router are co-located in the same device, the two protocols may be integrated into a single protocol like IKEv2. After completion of the tunnel establishment, the mobile node is able to communicate using both oCoA and nCoA by the end of Step 4.

**Step 3 (secure proactive handover):** The mobile node determines to switch to the new point of attachment by some means. Before the mobile node switches to the new point of attachment, it starts secure proactive handover by executing binding update of a mobility management protocol and transmitting subsequent data traffic over the tunnel. Based on the type of the target network the mobile is moving to and capability of the next hop router, this tunnel may not need to be secured also.

**Step 4 (secure proactive handover pre-switching phase):** The mobile node completes binding update and becomes ready to switch to the new point of attachment. The mobile executes the tunnel management protocol to delete the proactive handover tunnel. The mobile node caches nCoA even after deletion of the tunnel. The decision as to when the mobile node is ready to switch to the new point of attachment depends on a specific handover policy. This policy can include several metrics such as signal-to-noise ratio, available bandwidth, type of application being supported and network cost.

**Step 5 (switching):** It is expected that a link-layer handover occurs in this step. There are several ways to reduce the delay associated with link-layer handoff.

**Step 6 (secure proactive handover post-switching phase):** The mobile node executes the switching procedure. Upon successful completion of the switching procedure, the mobile node immediately restores the cached nCoA and assigns it to the physical interface attached to the new point of attachment. If the proactive handover tunnel was not deleted or disabled in Step 4, the tunnel is deleted or disabled as well. After this, direct transmission of data packets using nCoA is possible without using a proactive handover tunnel. By performing L2 switching and L3

configuration at the same time we can manage to reduce the delay to L3 configuration only. Timing of deletion of the existing tunnel will be mostly determined by layer 2 optimization.

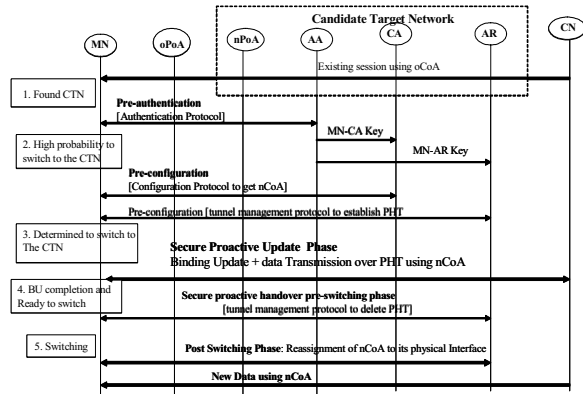


Figure 2. Stepwise MPA flow

## 4. Optimization Techniques

In the following subsections we describe some of the optimization issues and techniques need to be looked into in order to provide an optimized handover for a mobile experiencing rapid subnet and domain handover.

### 4.1. Network Discovery

Discovery of neighboring networking elements such as access points, access routers, authentication servers help expedite the handover process during a mobile's rapid movement between networks. By discovering the network neighborhood with a desired set of coordinates, capabilities and parameters the mobile can perform many of the operation such as pre-authentication, proactive IP address acquisition, proactive address resolution, and binding update while still in the previous network. There are several ways a mobile can discover the neighboring networks. The Candidate Access Router Discovery protocol [8] helps discover the candidate access routers in the neighboring networks. Given a certain network domain, SLP (Service Location Protocol) and DNS help provide address of the networking components for a given set of services in the specific domain. In some cases many of the network layer and upper layer parameters may be sent over link-layer management frames such as beacons when the mobile approaches the vicinity of the neighboring networks. IEEE 802.11u is considering issues such as discovering

neighborhood using information contained in link-layer. There is some proposal such as [18] that helps obtain these information about the neighboring networks from a mobility server using application layer protocols. When the mobile's movement is imminent, it starts the discovery process by querying a specific server and obtains the required parameters such as the IP address of the access point, its characteristics, routers, details of the authentication servers of the neighboring networks. At some point the mobile selects a specific candidate target network out of many probable networks and starts the pre-authentication process by communicating with the required entities in the candidate target networks.

### 4.2. Proactive IP Address Acquisition

In general IP address acquisition and configuration process takes of the order of few hundred milliseconds to few seconds depending upon the type of IP address acquisition process and operating system of the clients and servers. Since IP address acquisition is part of the handover process, it adds to the handover delay and thus it is desirable to reduce this timing as much as possible. There are few optimized techniques such as DHCP Rapid Commit [19], GPS-coordinate based IP address [20] that attempt to reduce the handover time due to IP address acquisition. However in all these cases the mobile obtains the IP address after it moves to the new subnet and incurs some delay because of the signaling handshake between the mobile node and the DHCP server. In the following paragraph we describe three techniques by which a mobile node can obtain the IP address proactively from the candidate target network.

In case of PANA-assisted (Protocol for carrying Network Authentication Access) [22] proactive IP address acquisition, the mobile node makes use of PANA messages to trigger the address acquisition process on the DHCP relay agent that co-locates with PANA authentication agent in the access router in the candidate target network. Upon receiving a PANA message from the mobile node, the DHCP relay agent performs normal DHCP message exchanges to obtain the IP address from the DHCP server in the candidate target network. This address is piggy-backed in a PANA message and is delivered to the client.

IKEv2-assisted proactive IP address acquisition works when an IPSec gateway and a DHCP relay agent are resident within each access router in the candidate target networks. In this case, the IPSec gateway and

DHCP relay agent in a candidate target network help the mobile node acquire the IP address from the DHCP server in the candidate target network. The MN-AR key established during the pre-authentication phase is used as the IKEv2 pre-shared secret needed to run IKEv2 between the mobile node and the access router. The IP address from the candidate target network is obtained as part of standard IKEv2 procedure, while using the co-located DHCP relay agent for obtaining the IP address from the DHCP server in the target network using standard DHCP. The obtained IP address is sent back to the client in the IKEv2 Configuration Payload exchange. In this case, IKEv2 is also used as the tunnel management protocol for a proactive handover tunnel.

As another alternative, DHCP may be used to proactively obtain an IP address from a candidate target network without relying on PANA or IKEv2-based approaches. It does so by allowing direct DHCP communication between the mobile node and the DHCP relay or DHCP server in the candidate target network. In this case, the mobile node sends a unicast DHCP message to the DHCP relay agent or DHCP server in the candidate target network requesting an address, with using the address associated with the current physical interface as the source address of the request. When the message is sent to the DHCP relay agent, the DHCP relay agent relays the DHCP messages back and forth between the mobile node and the DHCP server. In the absence of a DHCP relay agent the mobile can also directly communicate with the DHCP server in the target network. The broadcast option in client's unicast DISCOVER message should be set to 0 so that the relay agent or the DHCP server can send back the reply directly to the mobile using the mobile node's source address. In order to prevent malicious nodes from obtaining an IP address from the DHCP server, DHCP authentication should be used or the access router should install a filter to block unicast DHCP message sent to the remote DHCP server from mobile nodes that are not pre-authenticated.

Upon the mobile's entry to the new network, the mobile node can still use DHCP over its physical interface in the new network to get other configuration parameters such as SIP server, DNS server, etc., by using e.g., DHCP INFORM or can perform DHCP renew to renew the IP address lease. In order to maintain the DHCP binding for the mobile node and keep track of the dispensed IP address before and after the secure proactive handover, the same DHCP client identifier needs to be used for the mobile node during

the DHCP process in the previous network and target network. The DHCP client identifier may be the MAC address of the mobile node or some other identifier.

### 4.3. Proactive duplicate address detection

When the DHCP server dispenses an IP address, it updates its lease table, so that this same address is not given to another client for that specific period of time. At the same time the client also keeps a lease table locally so that it can renew when needed. In some cases where a network consists of both DHCP and non-DHCP enabled clients, there is a probability that another client within the LAN may have been configured with an IP address from the DHCP address pool. In such scenario the server does a duplicate address detection based on ARP (Address Resolution Protocol) or IPv6 Neighbor Discovery before assigning the IP address. This detection procedure may take up to 4 sec to 15 sec [21] and will thus contribute to a larger handover delay. In case of proactive IP address acquisition process, this detection is performed ahead of time and thus does not affect the handover delay at all and we reduce the handover delay factor associated with L3 configuration.

### 4.4. Proactive address resolution

During the process of pre-configuration the mobile can also obtain the address resolution mapping (ARP) of the neighboring nodes with whom it will need to communicate after attaching to the new network. These nodes may be the access router, authentication agent, configuration agent and correspondent node. There are several possible ways of performing such proactive address resolution.

As an example one can use an information service mechanism to resolve the MAC addresses of the nodes. This might require each node in the target network to involve in the information service discovery process so that the server of the information service can construct the database of proactive address resolution. One can extend the authentication protocol used for pre-authentication or the configuration protocol used for pre-configuration to support proactive address resolution. For example, if PANA is used as the authentication protocol for pre-authentication, PANA messages may carry AVPs used for proactive address resolution. In this case, the PANA authentication agent in the target network may perform address resolution for on behalf of the mobile node. One can define a new DNS resource record (RR)

to proactively resolve the MAC addresses of the nodes in the target network. This is probably not good because the mapping between domain name and MAC address is not stable in general. When the mobile node attaches to the target network, it installs the proactively obtained address resolution mappings without necessarily performing address resolution query for the nodes in the target network. Similarly, the nodes that reside in the target network and are communicating with the mobile node should also update their address resolution mappings for the mobile node as soon as the mobile node attaches to the target network. The above proactive address resolution methods could also be used for those nodes to proactively resolve the MAC address of the mobile node before the mobile node attaches to the target network. However, this is not useful since the nodes need to detect the attachment of the mobile node to the target network before adopting the proactively resolved address resolution mapping. A better approach would be integration of attachment detection and address resolution mapping update. This is based on gratuitously performing address resolution in which the mobile node broadcasts its ARP in the case of IPv4 or a Neighbor Advertisement in the case of IPv6 immediately after the mobile node attaches to the new network so that the nodes in the target network can quickly update the address resolution mapping for the mobile node.

#### 4.5. Proactive Tunnel management

After an IP address is proactively acquired from the DHCP server in a candidate target network, a proactive handover tunnel is established between the mobile node and the access router in the candidate target network. The mobile node uses the acquired IP address as the tunnel inner address and most likely it assigns the address to a virtual interface. The proactive handover tunnel is established using a tunnel management protocol. When IKEv2 is used for proactive IP address acquisition, IKEv2 is also used as the tunnel management protocol. Alternatively, when PANA is used for proactive IP address acquisition, PANA may be used as the secure tunnel management protocol. Once the proactive handover tunnel is established between the mobile node and the access router in the candidate target network, the access router also needs to perform proxy address resolution on behalf of the mobile node so that it can capture any packets destined to the mobile node's new address. Since mobile needs to be able to communicate with the correspondent node while in the previous network

some or all part of binding update and data from the correspondent node to mobile node need to be sent back to the mobile node over a proactive handover tunnel. Data from the mobile to the correspondent node may not need to be tunneled in the absence of ingress filtering. In order for the traffic to be directed to the mobile node after the mobile node attaches to the target network, the proactive handover tunnel needs to be deleted or disabled. The tunnel management protocol used for establishing the tunnel is used for this purpose. A link-layer trigger ensures that the mobile node is indeed connected to the target network and can also be used as the trigger to delete or disable the tunnel.

#### 4.6. Proactive Mobility Binding Update

Each mobility management scheme offers different types of binding update mechanisms. In case of Mobile IPv4 without route optimization, binding update is sent to home agent only, in case of Mobile IPv6, binding update is sent both to the home agent and correspondent host. In case of SIP-based terminal mobility the mobile sends binding update using ReINVITE to the correspondent host and REGISTER message to the Registrar. Based on the distance between the mobile and the correspondent node the binding update may contribute to the handover delay. SIP-fast handover [15] provides several ways of reducing the handover delay due to binding update. In case of secure proactive handover using SIP-based mobility management we rule out the delay due to binding update completely, as it takes place in the previous network. Thus this scheme looks more attractive when the correspondent node is too far from the communicating mobile node.

Although IP address acquisition and binding update are optimized, there may be some transient packets that can be lost during link-layer handover and until the traffic to be directed to the mobile node after attaching to the target network. Bicasting or buffering the transient packets at the access router can be used to minimize or eliminate packet loss. However, bicasting does not eliminate packet loss if link-layer handover is not seamlessly performed. On the other hand, buffering does not reduce packet delay. While packet delay can be compensated by playout buffer at the receiver side for streaming application, playout buffer does not help much for interactive VoIP application that cannot tolerate for large delay jitters. Thus it is still important to optimize the link-layer handover anyway.

#### 4.7. Link-layer security and mobility

Using the MPA-SA established between the mobile node and the authentication agent in a candidate target network, during the pre-authentication phase, it is possible to bootstrap link-layer security in the candidate target network while the mobile node is in the current network. One possible way of achieving link layer security is explained. These can be obtained in the following ways.

After the mobile node chooses a specific candidate network as the target network and switches to a point of attachment in the target network (which now becomes the new network for the mobile node), it executes a secure association protocol such as IEEE 802.11i 4-way handshake [802.11i] using the PMK in order to establish PTKs (Pair-wise Transient Keys) and GTKs (Group Transient Keys) used for protecting link-layer packets between the mobile node and the point of attachment. No additional execution of EAP authentication is needed here.

While the mobile node is roaming in the new network, the mobile node only needs to perform a secure association protocol with its point of attachment point and no additional execution of EAP authentication is needed either. Integration of MPA with link-layer handover optimization mechanisms such as 802.11r can be archived this way. The mobile node may need to know the link-layer identities of the point of attachments in the candidate target network to derive TSKs. If PANA is used as the authentication protocol for pre-authentication, this is possible by carrying Device-Id AVPs in the PANA-Bind-Request message sent from the PAA [22], with each AVP containing the BSSID of a distinct access point. When the mobile node initially attaches to a network, network access authentication would occur regardless of the use of MPA.

### 5. Implementation and Results

This section describes details of a specific implementation. It also provides the evaluation results of optimized hand-off with MPA and compares it with non-MPA-based handover. Figure 3 shows the experimental testbed and associated network elements.

There are three networks defined in the implementation environment. Network 1 is old point of

attachment (oPoA), Network 2 is new point of attachment (nPoA), and network 3 is where the correspondent node (CN) resides. The mobile is initially in Network 1 and starts communicating with the correspondent node. Network 1, network 2, and network 3 do not need to be adjacent. In the implementation scenario however, network 1, network 2 and network 3 are one hop away. In the event of mobile's movement, a specific Mobility Management Protocol (MMP) can take care of continuity of streaming traffic set up by the peer-to-peer application.

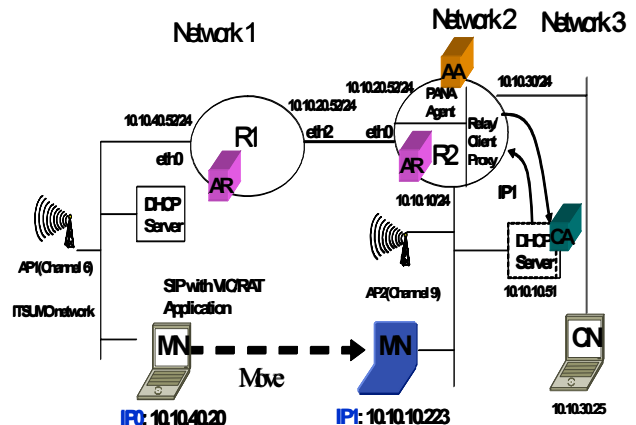


Figure 3: Experimental Testbed

Network 1 consists of DHCP Server 1, access point (AP) 1 and Access Router 1. Network 2 consists a DHCP Server 2, AP 2 and Access Router 2. AP 1 and AP 2 are 802.11 wireless LAN access points. Router 2 also works as a PANA Authentication Agent (PAA) [22] and a DHCP Relay Agent for Network 2, but they can be separated. DHCP relay-agent also acts like a Configuration Agent (CA) that helps obtain the IP address for the mobile proactively from the neighboring target network. Network 3 consists of a Correspondent Node (CN) that communicates with the mobile node in Network 1. Both the correspondent node and mobile node are equipped with Mobile SIP client and PANA Client (PaC). Mobile Node (MN) uses 802.11 wireless LAN as the access method and can communicate via AP 1 before it moves to Network 2 where it communicates via AP 2. In this specific case, the Mobility Management Protocol (MMP) is SIP Mobility (SIP-M), configuration protocol is DHCP, authentication agent (AA) is PAA, configuration agent (CA) is DHCP Relay Agent and Access Router (AR) is Router 2 that can provide IP-in-IP tunneling functions. Thus the mobile has the ability to set up a tunnel interface and de-tunnel the packets

sent over the tunnel between the router 2 and the mobile. The protocol flow for MPA along with the results of our implementation environment is described in Figure 3. As the MN bootstraps, it associates with

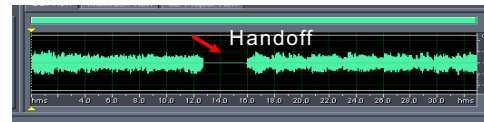
device drivers under two operating systems primarily Linux and Windows. This total timing includes the steps for scanning, probe request/response, association and authentication process. However, we significantly reduced the delay due to Layer 2 by implementing HOSTAP driver in the roaming mode, and minimized the scanning time by providing the access point parameters of the target network during the handover. We took advantage of network discovery mechanism that provides the details of the access points in the neighboring networks including the channel number and Ethernet addresses.

Table 1: Measured L2 hand-off delay

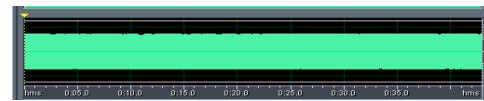
H/W - OS	L2 Handoff
AiroNet +Linux	200 – 300 ms
Orinoco+Linux	100 – 160 ms
DLink +Linux	400 – 600 ms
Centrino + Linux (Passive)	300 ms
Orinoco +Windows	250 ms
Hostap (Managed)	14 ms

A similar scheme such as [14] can also be implemented to reduce the layer 2 delay. As observed in Figure 3, total handoff delay in MPA-based scheme is limited to 14 ms. Since the spacing between the audio packets is about 16 ms, we lost only 1 packet which is less than 2% and is within allowable limit. We also observed that there is a tradeoff between deletion of the tunnel before mobile's handoff and its deletion after the handoff. In the former case, packets get dropped in the target network, while in the later case the packets get dropped in the previous network. A buffering mechanism is needed to retrieve the transient packets those are lost during the handoff. Although buffering mechanism may not help reducing the handoff delay, it will help in reducing the packet loss and may help beneficial for streaming and data traffic. A dynamic buffering mechanism can be deployed at the router in the target network to take care of the transient packet loss. Design of a specific buffering mechanism to take care of the packet loss is beyond the scope of this paper. However schemes similar to [23] [24] can be used to provide buffering mechanism at the target router. For comparison purposes, we also experimented with non-MPA scenario that does not provide any proactive handover mechanism as such but follows standard handover procedure of obtaining the IP address, performing the

authentication and sending the binding update after the mobile moves to the new subnet. In case of non-MPA-based handoff scenario, handover delay and attributed packet loss take place because of L2 handover during the movement, IP address assignment, post-authentication, and mobility binding update. Especially DHCP takes long time to complete the detection of duplicate of IP address in the network and binding update can take a long time if the correspondent node is too far from the mobile node. In our testbed non-MPA-based handover took up to 4 seconds delay due to all the above factors. Streaming traffic on the correspondent host was generated using a CODEC that has a spacing of 20 ms between the packets. We observed that approximately 200 packets were lost in the absence of MPA-based proactive scheme. Figure 7 shows a snapshot of audio being received at the mobile during its handover for both MPA-based and Non-MPA-based handover.



Non-MPA scheme



Optimized MPA scheme

Figure 7: Audio output at the mobile (MPA/Non-MPA)

In this example network, candidate protocols can always be replaced by the other protocols, for example, mobility management protocol that provides binding update can be replaced by Mobile IPv4 or Mobile IPv6. Similarly the tunnel management protocol can always be replaced by IKEv2 and IPsec tunnel mode. It is normal to assume the performance values will be different based on the type of candidate protocols used. In this case, MPA scheme has been experimented with a single interface only, but it can very well be extended to support a mobile equipped with multiple interfaces that moves between heterogeneous access networks such as 802.11 and CDMA or GPRS. In case of heterogeneous access network, mobile has the option of performing the authentication using either the old interface or the new interface (e.g., 802.11 or CDMA in case when mobile moves from LAN to WAN). Mobile can obtain the IP

address for its new interface in the background while it is still communicating with using its old interface.

## 6. Conclusions

In this paper we have presented a framework for a secured proactive handover mechanism, discussed the associated optimization techniques, and explained the experimental results from a laboratory implementation. MPA framework takes advantage of the available network discovery mechanisms and thus obtains the required parameters of the networking elements of the target networks before the handoff occurs. Obtaining these parameters help perform the secured proactive handover and thus reduces the delay and packet loss during the handover to a level that is acceptable for interactive VoIP and streaming traffic. A comparison with standard handoff mechanism that does not use MPA-based scheme shows that we can get marked performance improvement during rapid handoff using MPA assisted optimized proactive handoff scheme.

## 7. Acknowledgement

Authors would like to acknowledge Victor Fajardo, and Provin Gurung for their help during implementation.

## 8. References

- [1] C. Perkins et al "IP Mobility Support for IPv4", RFC 3344, August 2002
- [2] D. Johnson et al, "Mobility Support in IPv6", RFC 3775
- [3] T. Kivinen et al "Design of the MOBIKE protocol", draft-ietf-mobike-design-01 (work in progress), January 2005.
- [4] R. Moskowitz et al, "Host Identity Protocol", draft-ietf-hip-base-01 (work in progress), October 2004.
- [5] H. Schulzrinne, E. Wedlund, "Application Layer Mobility Using SIP", MC2R.
- [6] K. Malki, "Low latency Handoffs in Mobile IPv4", draft-ietf-mobileip-lowlatency-handoffs-v4-09 (work in progress), June 2004.
- [7] R. Koodli, "Fast Handovers for Mobile IPv6", draft-ietf-mipshop-fast-mip6-03 (work in progress), October 2004.
- [8] M. Liebsch, "Candidate Access Router Discovery", draft-ietf-seamoby-card-protocol-08 (work in progress), September 2004.
- [9] A. Campbell et al., "Design, Implementation, and Evaluation of Cellular IP" IEEE Personal communication August 2000.
- [10] R. Ramjee et al, "HAWAII: A Domain-based Approach for Supporting Mobility in Wide-area Wireless networks"
- [11] S. Das et al, "IDMP: An Intra-Domain Mobility Management Protocol for Next Generation Wireless Networks", IEEE Wireless Communication Magazine October 2000.
- [12] P. Calhoun et al, "Mobile IPv4 Regional Registration", draft-ietf-mobileip-reg-tunnel-09 (work in progress), July 2004.
- [13] Yokota et al, "Link Layer Assisted Mobile IP Fast Handoff Method over Wireless LAN Networks", Proceedings of ACM Mobicom 2002.
- [14] S. Shin et al, "Reducing MAC Layer Handoff Latency in IEEE 802.11 Wireless LANs", MOBIWAC Workshop
- [15] A. Dutta et al, "Fast handoff Schemes for Application Layer Mobility Management", PIMRC 2004.
- [16] Y. Gwon et al, "Fast Handoffs in Wireless LAN Networks using Mobile initiated Tunneling Handoff Protocol for IPv4 (MITHv4)", Wireless Communications and Networking 2003, January 2005.
- [17] A. Dutta et al, "Secured Universal Mobility", WMASH 2004.
- [18] F. Anjum et al, "A proposal for MIH function and Information Service", A contribution to IEEE 802.21 WG, January 2005.
- [19] P. Kim et al, "Rapid Commit Option for DHCPv4", draft-ietf-dhc-rapid-commit-opt-05 (work in progress), June 2004
- [20] A. Dutta et al, "GPS-IP based fast-handoff for Mobiles", NYMAN
- [21] J. Vatn et al "The effect of using co-located care-of-address on macro handover latency" International Teletraffic Conference, 1998
- [22] D. Forsberg et al, "Protocol for Carrying Authentication for Network Access (PANA)", draft-ietf-pana-pana-07 (work in progress), December 2004.
- [23] C-H Lee, D. Lee, J. W. Kim, "Seamless MPEG-4 Video Streaming Over Mobile IP-enabled Wireless LAN", Network Research Workshop, 2004, 18<sup>th</sup> APAN meeting
- [24] H. Yu, K. Park, Y. Chae, H. Jung, "Inter-subnet Handoff Regional Tunnel Management", ICT 2000