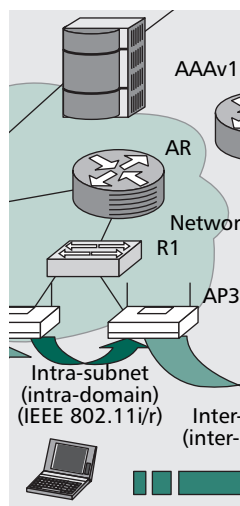


# MEDIA-INDEPENDENT PRE-AUTHENTICATION SUPPORTING SECURE INTERDOMAIN HANDOVER OPTIMIZATION

ASHUTOSH DUTTA, DAVID FAMOLARI, AND SUBIR DAS, TELCORDIA TECHNOLOGIES  
YOSHIHIRO OHBA, VICTOR FAJARDO, KENICHI TANIUCHI, AND RAFAEL LOPEZ,  
TOSHIBA AMERICA RESEARCH  
HENNING SCHULZRINNE, COLUMBIA UNIVERSITY



The authors categorize several types of handover, describe handover delay components, and propose a handover optimization framework called Media Independent Pre-authentication.

## ABSTRACT

Handovers may cause delays and packet losses that affect real-time communication performance. Mobility protocols at several layers are designed to support handover, but they need to be optimized to ensure high-quality application performance. Existing optimization techniques are not sufficient to take care of interdomain and intertechnology handovers involving different access technologies, such as Wi-Fi, GSM, CDMA, and WiMAX. We categorize several types of handover, describe handover delay components, and propose a handover optimization framework called Media Independent Pre-Authentication that can provide optimizations for interdomain and intertechnology handover in a manner that is transparent to mobility management protocols. In addition, we also present experimental results demonstrating that this framework can achieve a significant reduction in handover delays for both network-layer and application-layer mobility management protocols.

## INTRODUCTION

Handover is a process by which a mobile node moves from one point of network attachment to another. Handovers can be classified as either homogeneous or heterogeneous. Heterogeneous handover includes either movement between different types of access technologies or movement across different administrative domains. As the diversity of available networks increases, it is important that mobility technologies are agnostic to link layer technologies, and can operate in an optimized and secure fashion without incurring unreasonable delay and complexity. Supporting handovers across heterogeneous access networks, such as IEEE 802.11 (Wi-Fi), Global System for Mobile Communications (GSM),

code-division multiple access (CDMA), and WiMAX is a challenge, as each has different quality of service (QoS), security, and bandwidth characteristics. Similarly, movement between different administrative domains poses a challenge since mobiles need to perform access authentication and authorization in the new domain. In order to provide desirable QoS for interactive voice over IP (VoIP) and streaming traffic, one needs to limit end-to-end delay, jitter, and packet loss to within acceptable levels. However, our previous experiments [1] suggest that in the absence of any optimization technique, handover delays can range from 3 to 15 s based on the type of access network, type of handover, and type of mobility protocol. Thus, it is desirable to devise a mobility optimization technique that can reduce these delays and is not tightly coupled to a specific mobility protocol.

In order to provide an optimized heterogeneous and interdomain handover solution, it is essential to determine the key functions that contribute to handover delay. In this article we describe different types of handover involving heterogeneous access technologies and diverse administrative domains, and investigate the handover components that contribute to delay, packet loss, and jitter. We discuss several challenges during heterogeneous and interdomain handover, and highlight how current mobility optimization techniques are too tightly coupled to specific mobility protocols and not suitable for interdomain handoff optimization. We then propose a media-independent fast handover framework to support interdomain handoff optimization, and present experimental results of this framework for interdomain handoff using application- and network-layer mobility protocols.

We present the handover taxonomy and discuss handover delays. Related optimization tech-

When a mobile's movement is confined to movement within an administrative domain, it is called intra-domain movement. An intra-domain movement may also involve intra-subnet, inter-subnet, intra-technology and/or inter-technology handovers as well.

niques that demonstrate the need for an optimization framework for interdomain handoff are described. We also provide an overview of Media-Independent Pre-Authentication (MPA). Experimental results are summarized while deployment issues are detailed. Finally, we conclude the article.

## TAXONOMY OF HANDOVER TYPES

As previously stated, handover is a process by which a mobile node moves from one point of attachment to another point of attachment. There are three primary characteristics of the networks that can serve to categorize handovers: subnets, administrative domains, or access technologies. Thus, a handover can be categorized into these three classes. Mobile devices may move between any combinations of these three elements, as discussed below.

### INTERTECHNOLOGY

A mobile may be equipped with multiple interfaces supporting different technologies (e.g., Wi-Fi, GSM, CDMA, WiMAX). Intertechnology handovers occur when the two points of attachment use different access technologies. It may be preferable to communicate using only one interface at a time in order to conserve power. During the handover, the mobile may move out of the footprint of one access technology (e.g., Wi-Fi) and into the footprint of a different one (e.g., CDMA). This will trigger switching the communicating interface on the mobile. This type of intertechnology handover is often referred to as *vertical handover*, where the mobile moves between two different cell sizes belonging to different access networks. An intertechnology handover may also affect the QoS of applications, since different access networks can offer significantly different bandwidth and delay profiles.

### INTRATECHNOLOGY

An intratechnology handover occurs when a mobile moves between points of attachment supporting the same type of access technology, such as between two Wi-Fi access points or two cell sites supporting CDMA 1xRTT and CDMA EVDO. In this scenario a mobile may be equipped with a single interface (with multiple PHY types of the same technology) or multiple interfaces. An intratechnology handover may involve intrasubnet or intersubnet movement and thus may need to change its layer 3 identifier, depending on the type of movement.

### INTERDOMAIN

An interdomain handover occurs when the two points of attachment belong to different administrative domains. For the purposes of roaming, we define a domain as a set of network resources managed by a single administrative entity that authenticates and authorizes access for the mobile nodes. An administrative entity may be a service provider, an enterprise, or an enterprise in an organization. An interdomain handover may also involve either an inter- or intratechnology handover. Thus, it is very likely that an interdomain handover will include an intersubnet handover

since subnets are not typically shared by two administrative domains. Interdomain handover requires authorization for acquisition or modification of resources assigned to the mobile. The authorization process normally needs to interact with a central authority in a domain.

### INTRADOMAIN

When a mobile's movement is confined to movement within an administrative domain, it is called intradomain movement. Intradomain movement may also involve intrasubnet, inter-subnet, intratechnology, and/or intertechnology handovers as well.

### INTERSUBNET

An intersubnet handover occurs when the two points of attachment belong to different subnets. Such movement will require that the mobile device acquire a new IP address and possibly undergo a new security or authentication procedure. Intersubnet handovers may occur along with either inter- or intradomain and inter- or intratechnology handovers.

### INTRASUBNET

An intrasubnet handover occurs when the two points of attachment belong to the same subnet. This is typically a link layer handover between two access points in enterprise wireless LAN (WLAN) networks, or between different cell sectors or cell sites in cellular networks. This type of handover is typically administered by the radio network and normally requires no additional authentication, security, or higher-layer configuration procedures.

Some common handover categorizations are discussed below. An intertechnology, interdomain, intersubnet handover occurs when a dual-mode Wi-Fi/CDMA device transitions from the CDMA network of one service provider to the Wi-Fi network of another provider, say a coffee shop. For example, a device that enters a coffee shop and transfers its ongoing sessions from a CDMA network to the Wi-Fi network provided and managed by the coffee shop is an example of such a handover.

Another common handover type is intertechnology, intradomain, intersubnet. This case is similar to the one above; however, the Wi-Fi network is owned and operated by the same provider as the CDMA network. This use case is typical of emerging fixed-mobile convergence efforts that aim to allow customers to carry calls on the cellular network as well as on Wi-Fi networks located in enterprises, homes, and coffee shops but managed and operated by the cellular provider.

Intratechnology, interdomain handovers are also common and include cases where a device moves from one administrative domain to another using the same access technology. Handovers between cellular networks' roaming partners are a good example of such handovers. These handovers typically involve intersubnet handovers as well.

Finally, intratechnology, intradomain, intersubnet handovers involve cases where a mobile device with a single interface moves from one subnet to another within the same provider network. Enter-

prise workers who carry their Wi-Fi enabled laptops from one area of the Wi-Fi network to another, or may transition from the Wi-Fi network assigned to the marketing department to that assigned to the engineering department may experience this type of handover.

## HANDOVER DELAY

Several subcomponents within each layer contribute to the overall handover delay.

### LAYER 2 DELAY

Depending on the access type (e.g., 802.11, CDMA), the mobile goes through several steps, adding delay in each step, before the new layer 2 link is established. As an example, an 802.11 link goes through the process of scanning, authentication, and association during the attachment to the new access point. Similarly, other access networks such as CDMA and Generic Packet Radio Service (GPRS) networks go through a series of state transitions during their association to the new point of attachment. Depending on the nature of the handover, application traffic may or may not be resumed once the layer 2 processes have taken place. For intrasubnet cases, when no layer 3 configuration is necessary, layer 2 delays constitute the lion's share of the overall handover delay.

### LAYER 3 DELAY

Once a device has completed the layer 2 procedures, it may be necessary to initiate a layer 3 transition process. This process may include several steps, such as acquiring a new IP address, detecting a duplicate address, ARP update, and subnet-level authentication. IP address acquisition methods are different based on the version of IP in use (e.g., IPv4, IPv6) and the access network. Configuration protocols such as DHCPv4, DHCPv6, PPP or stateless auto-configuration incur different delays for IP address acquisition process. After a layer-3 transition is complete, other functions such as the binding update from the mobile and media redirection at the sending host also contribute to handoff delay.

### APPLICATION LAYER DELAY

Application layer delay is the delay needed to reestablish or modify mid-session application layer properties such as IP address using Session Initiation Protocol (SIP) Re-INVITE or codec parameters involving end-to-end applications. These procedures ensure that application packets will be delivered to the new IP destination.

In interdomain mobility, the delay introduced by authentication and authorization adds to the handover latency, and impairs the seamlessness of ongoing multimedia sessions. The authentication and authorization procedure may include several round-trip message exchanges (e.g., Extensible Authentication Protocol [EAP] authentication [2]) between the mobile and the authentication, authorization, and accounting (AAA) server. Although it depends on the network architecture, in most cases these signaling messages need to reach the AAA server in the home domain before access to the network service can be granted to the mobile in the new

network. Ruckforth and Linder [3] show that the delays associated with interdomain mobility could amount to 5 s due to authentication and authorization.

## RELATED WORK IN HANDOFF OPTIMIZATION

Different types of handover are subject to different amounts of delay. For example, an intrasubnet, intratechnology handover will take much less time than an intersubnet, intertechnology handover, because the mobile goes through fewer state transitions during the handover process. Fathi *et al.* provide a survey of available optimized mobility management solutions at different layers [4] that attempt to reduce handover delay and mitigate packet loss. Mobility optimization mechanisms discussed in [5, 6] are defined for Mobile IPv4 and Mobile IPv6, respectively, that allow neighboring access routers to communicate and carry information about mobile terminals to accelerate the handover process. These protocols are considered "helpers" or mobility optimization mechanisms. The Candidate Access Router Discovery (CARD) protocol [7] is designed to discover neighboring access routers. The Context Transfer Protocol (CTP) [8] carries state that is associated with the services provided for the mobile terminal among access routers. However, existing mobility optimization mechanisms fall short in supporting interdomain mobility. First, 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 SIP-based mobility [9] for Mobile IPv6 [10] or the Host Identity Protocol (HIP).

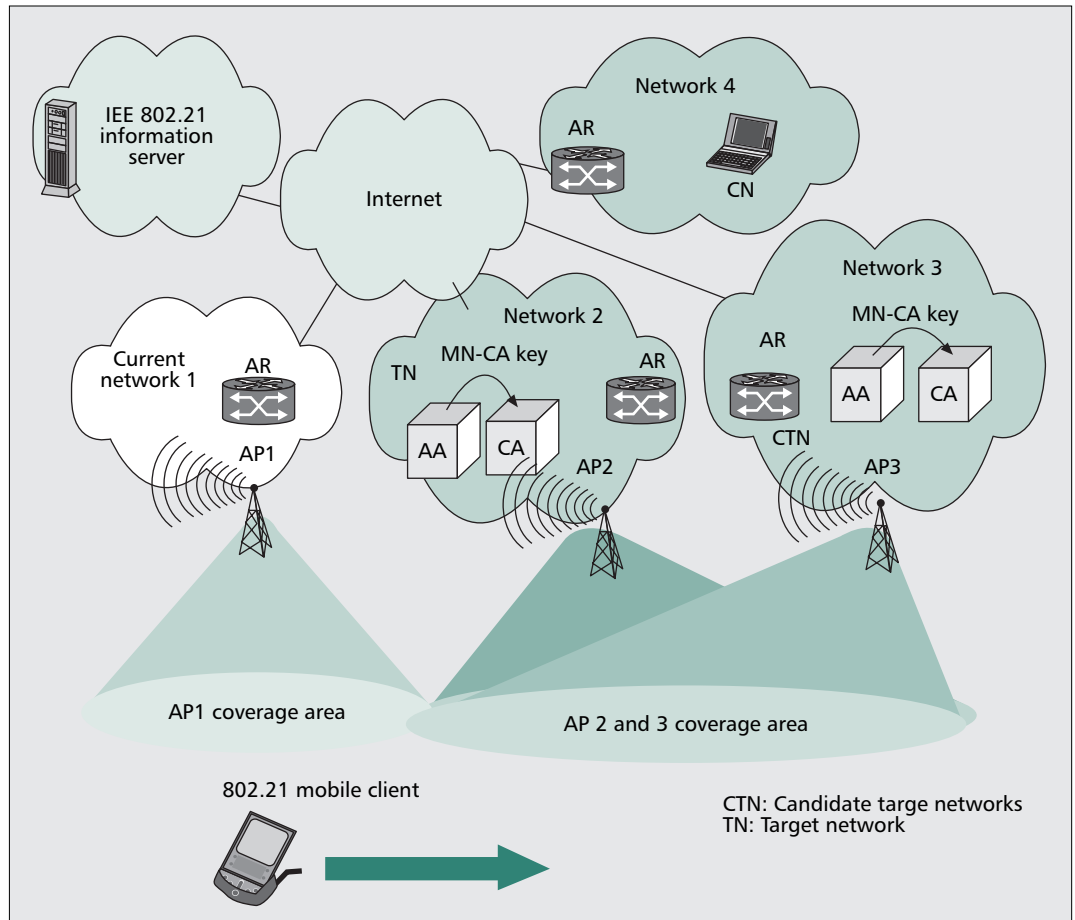
Second, there is no existing mobility optimization mechanism that easily supports handovers across administrative domains without assuming a pre-established security association. Third, a mobility optimization mechanism needs to support terminals that can connect through multiple interfaces as well as terminals that only have one interface. Finally, a mobility optimization technique should be able to provide value even if the mobility protocol is different in each domain. The existing optimization techniques in their current form do not adequately support handover involving multiple administrative domains. Thus, there is a need for mobility optimization mechanisms that work with any mobility management protocol and can support interdomain optimization without assuming any pre-established security arrangement between the domains. We propose a media-independent pre-authentication framework that addresses these drawbacks, and accelerates authentication and authorization.

## OVERVIEW OF MEDIA PRE-AUTHENTICATION

Media-Independent Pre-Authentication (MPA) is a mobile-assisted, secure handover optimization scheme that works over any link layer and

Different types of handover are subject to different amount of delays. For example, an intra-subnet, intra-technology handover will take much less time than an inter-subnet, inter-technology handover.

With MPA, a mobile node securely obtains an IP address and other configuration parameters for a Candidate Target Network (CTN), but is also able to send and receive IP packets using that IP address before it attaches to the CTN.



■ Figure 1. MPA-based deployment scenario.

with any mobility management protocol. With MPA, a mobile node securely obtains an IP address and other configuration parameters for a candidate target network (CTN), but is also able to send and receive IP packets using that IP address before it attaches to the CTN. The CTN is one of the neighboring networks into which the mobile is likely to move. 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 (CoA) before performing a handover at the link layer (assuming the mobile node can maintain connectivity with the serving network during this time).

MPA provides four basic procedures that optimize handover for a mobile device that has connectivity to the serving network but is not yet attached to the CTN. The serving network is the network that currently serves the mobile. The first procedure is referred to as *pre-authentication* and establishes a security association with the CTN to secure subsequent protocol signaling. The second procedure is referred to as *pre-configuration* and securely executes a configuration protocol to obtain an IP address and other parameters from the CTN. The third procedure executes a tunnel management protocol that establishes a proactive handover tunnel (PHT) between the mobile device and an access router in the CTN over which IP packets, including binding updates as well as data packets, can

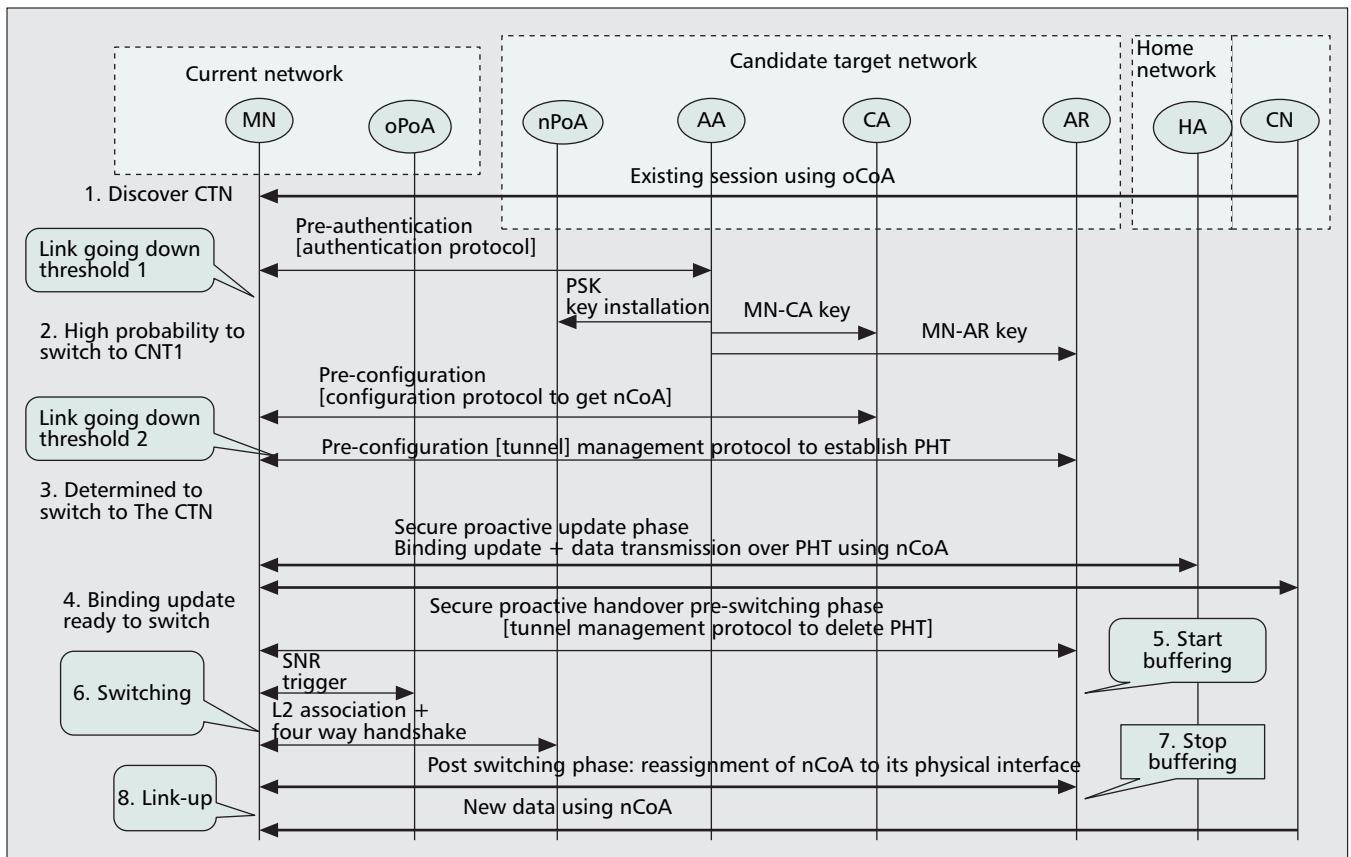
travel. Packets transmitted over the tunnel contain the IP address acquired during the pre-configuration phase as part of the inner tunnel address. Finally, the fourth procedure deletes the PHT immediately before attaching to the CTN and reassigns the inner address of the deleted tunnel to its physical interface immediately after the mobile device attaches to the target network. The final two procedures are collectively referred to as *secure proactive handover*.

The third procedure described above makes it possible for the mobile to complete the higher-layer handover before starting link layer handover. This means that the mobile is able to perform all the higher-layer configuration and authentication procedures before layer 2 connectivity to the CTN is established. Packets diverted to the mobile device before the binding update is completed are delivered via the tunnel. This can significantly reduce handover delays.

### MPA FUNCTIONAL ELEMENTS

In the MPA framework each CTN hosts an authentication agent (AA), configuration agent (CA), and access router (AR), distributed over one or more network devices. Figure 1 shows an example of MPA deployment.

The 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



■ **Figure 2.** Media-independent pre-authentication communication flow.

(security association). The authentication protocol must be able to derive a key between the mobile node and the authentication agent, and should be able to mutually authenticate. The authentication protocol should be able to interact with an AAA protocol such as RADIUS or Diameter [11] to carry authentication credentials to an appropriate authentication server in the AAA infrastructure. The derived key is used to further derive keys for protecting message exchanges that are used for preconfiguration and secure proactive handover. Other keys that are used for bootstrapping link or network layer ciphers may also be derived from the MPA-SA. A protocol that can support the EAP framework would be suitable as an authentication protocol for MPA. Protocol for Carrying Authentication for Network Access (PANA) is one such example.

The configuration agent (CA) is responsible for one part of preconfiguration, securely executing a configuration protocol to deliver an IP address 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 responsible for securely executing a tunnel management protocol to establish a proactive handover tunnel to the mobile node. The signaling messages associated with the configuration protocol must be protected using a key derived from the MPA-SA. IP packets transmitted over the proactive

handover tunnel should also be protected using a key derived from the MPA-SA.

### MPA PROTOCOL FLOW

Figure 2 shows an MPA-based protocol flow. Assume that the mobile node is already connected to a point of attachment referred to as the old point of attachment (oPoA) and assigned an old CoA (oCoA). Throughout the communication flow, a data packet should not be lost except for the period during the layer 2 switching procedure in step 5, but MPA can help minimize the packet loss during this period with the help of IEEE 802.21's media-independent information service [11] by way of its information service (IS), event service (ES), and command service (CS).

**Pre-Authentication Phase** — The mobile finds a CTN through a discovery process, such as IEEE 802.21 [12], and obtains the address and capabilities of the AA, CA, and AR in the CTN. The mobile pre-authenticates 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, an MN-CA key and an MN-AR key, which are used to protect subsequent signaling messages of a configuration protocol and a tunnel management protocol, respectively. The MN-CA and MN-AR keys are then securely delivered to the configuration agent and access router, respectively. Layer 2 pre-authentication can be initiated at this stage.

In the case of intra-technology handover, the mobile moves between 802.11-based networks, whereas for inter-technology handover the mobile moves between an 802.11-based network and a CDMA-based network.

**Preconfiguration Phase** — The mobile node realizes that its point of attachment is likely to change from oPoA to a new one, say, nPoA. It then performs preconfiguration, 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 CTN. The access router uses 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 tunnel inner address, respectively. The signaling messages of the preconfiguration protocol are protected using the MN-CA and MN-AR keys. When the configuration and access router are collocated in the same device, configuration and tunnel management may be performed by a single protocol such as IKEv2. After completion of tunnel establishment, the mobile is able to communicate using both oCoA and nCoA by the end of step 4.

**Secure Proactive Handover Main Phase** — Before the mobile switches to the nPoA, it starts secure proactive handover by executing the binding update operation of a mobility management protocol and transmitting subsequent data traffic over the tunnel. In some cases it may cache multiple nCOA addresses and perform simultaneous binding with the corresponding host (CH) or home agent (HA).

**Secure Proactive Handover Preswitching Phase** — The mobile completes the binding update and becomes ready to switch to the nPoA. The mobile may execute the tunnel management protocol to delete or disable the proactive handover tunnel and cache nCoA after deletion or disabling of the tunnel. A buffering module at the new AR (nAR) begins to buffer the packets (start-buffering) when it receives the tunnel-delete signal. The mobile sends an explicit signal to stop buffering and flush the packets after the mobile connects to the nPoA.

The decision on when the mobile switches to the nPoA depends on the handover policy. In general, mobile-controlled or network-controlled policies can be used to trigger the handoff. The mobile's signal quality, location, communication cost, and QoS on the received traffic are some factors that can determine the handoff policy. Results presented in this article are based on signal-to-noise ratio (SNR).

**Switching Phase** — It is expected that a link layer handover occurs in this step. During this phase, any layer 2 security association, including EAP-based authentication and 802.11i related four-way handshake, may take place. Normally, layer 2 pre-authentication is taken care of by the layer 2 built-in pre-authentication support. In this scheme layer 3 pre-authentication can bootstrap layer 2 authentication, leaving only the four-way handshake during this phase.

**Secure Proactive Handover Post-Switching Phase** — The mobile executes the switching procedure. Upon successful completion of the switching procedure and layer 2 association, the mobile immediately

restores the cached nCoA and assigns it to the physical interface attached to the nPoA. If the proactive handover tunnel was not deleted or disabled in step 4, the tunnel can be deleted or disabled in this phase as well. After this, direct transmission of data packets using nCoA is possible without using a proactive handover tunnel.

Several deployment issues associated with the MPA framework for interdomain handoff are discussed later.

## EXPERIMENTAL RESULTS AND ANALYSIS

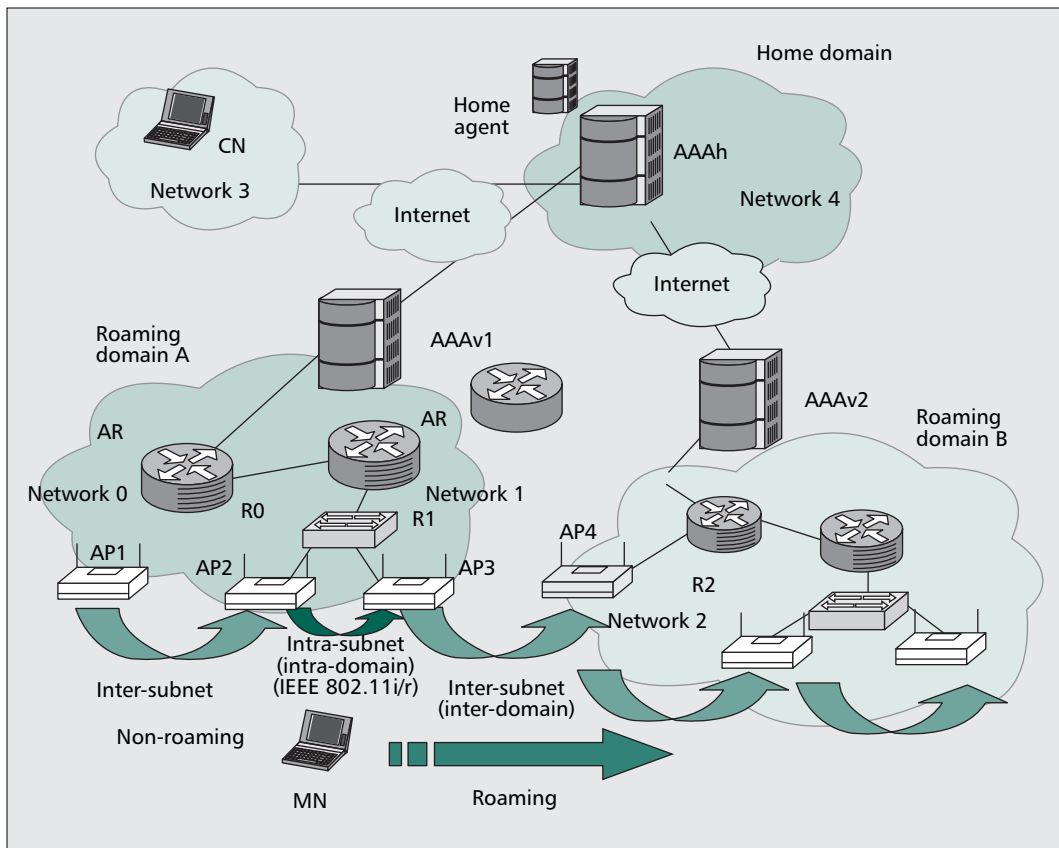
In this section we highlight experimental results using two mobility protocols, SIP-based mobility [9] and MIPv6 [10], for both intertechnology, interdomain and intratechnology, interdomain handovers. In the case of intratechnology handover the mobile moves between 802.11-based networks, whereas for intertechnology handover the mobile moves between an 802.11-based network and a CDMA-based one.

Figure 3 shows the basic topology of the experimental testbed. The testbed emulates two different visited domains and a home domain. Each visited domain has several subnetworks. Initially, the mobile resides in network 1. The mobile moves from one visited domain to another domain and in the process changes its subnet. Network 1 is the oPoA where the mobile node (MN) initially resides prior to handover. Network 2 is the nPoA, network 3 is where the CN resides, and finally, network 4 is where the HA resides. In MPA for MIPv6, the CN starts a Real-Time Transport Protocol (RTP) session with the MN while the MN is in network 1 via the HA using an MIPv6 tunnel. MPA creates a proactive handover tunnel between the MN and R2 in network 2. This is an IPsec tunnel in Encapsulating Security Payload (ESP) mode, and we use the protocol to carry PANA [9] for dynamically establishing and terminating the IPsec tunnel. Before the handoff, the MIPv6 tunneled traffic between the MN and HA goes through the IPsec tunnel created by MPA with IPsec policy settings. When the configuration agent and router collocate, a single protocol such as IKEv2 can take care of both functions (e.g., configuration and tunnel management).

We have also used MPA with application layer mobility such as SIP Mobility (SIP-M) [9]. Initially, the MN associates itself with AP3 and obtains an IP address from Dynamic Host Configuration Protocol (DHCP) server 1 in network 1. The IP address obtained in network 1 is the old oCoA. The CN establishes a SIP session with the MN and sends RTP traffic. An IP-in-IP transient tunnel is created between MN and R2 to route the traffic before handoff. Similar to MIPv6, an optional packet buffering exists in R2 to assist with packet loss during handover. We describe two types of handover with which we have experimented, namely intratechnology/interdomain and intertechnology/interdomain.

### INTRATECHNOLOGY AND INTERDOMAIN

In this case, to test intratechnology and interdomain handover, we used 802.11 as the access network in both domains. Table 1 shows the



■ **Figure 3.** Interdomain mobility optimization testbed.

mean value of measurements taken from five test samples. Average packet loss is the number of packets that failed to reach the MN during layer 2 and 3 handoff periods. The average interpacket arrival interval is 16 ms and represents the average time interval between consecutive RTP packets as they arrive at the MN before the handover. However, the average interpacket arrival time during handover is the amount of time between the last RTP packet received by the MN before handover and the first RTP packet received by the MN after handover. This includes the binding update signaling (SIP re-INVITE and MIPv6 binding update) as well as any signaling for buffering. Packet jitter is the interpacket time during handover minus average interpacket arrival interval.

This table provides a measurement of the average additional delay incurred because of the handover process. Buffering at R2 is an optional mechanism that buffers in-transit packets at R2 on behalf of the MN during the handoff period. “Buffered packets” is the number of packets that are buffered and eventually forwarded to the MN after handoff when buffering is enabled. PANA is used as a pre-authentication protocol to establish an SA between the MN and network 2. Also, handover signaling information is carried by PANA messages after successful pre-authentication. RO is the MIPv6 route optimization where the CN sends RTP packets directly to the MN’s nCoA, bypassing the HA. As observed from the experimental analysis, MPA provides zero packet loss and reduces layer 2 delay to 4 ms

compared with 3 s delay without optimization as observed in [1].

### INTERTECHNOLOGY AND INTERDOMAIN

Handoff involving interdomain and heterogeneous access (e.g., CDMA, 802.11) can take place in many ways. In a reactive scenario the second interface comes up when the link to the first interface goes down. This gives rise to undesirable packet loss and handoff delay. In the second scenario the second interface is being prepared while the mobile still communicates using the first interface. Preparation of the second interface should include setup of all the required state and security associations. After the preparation, the mobile can decide to use the second interface as the active interface. This results in fewer packet losses as it uses make-before-break techniques. As part of the MPA experiment, we added new optimization techniques such as faster link down detection and a copy forwarding technique at the access router to help reduce in-transit packet loss during the handover. Compared to nonoptimized handover that may result in delay up to 15 s and 1000 lost packets during handover from WLAN to CDMA, we achieved 0 packet loss and 50 ms handoff delay between the last prehandoff packet and first post-handoff packet. However, the copy forwarding caused, on average, about 10 duplicate packets, but these duplicate packets are easily discarded by application layer protocols. In the following section we explain how MPA can provide layer 2 security optimization during interdomain handover.

Currently, IEEE 802.11i cannot provide layer 2 pre-authentication during inter-domain mobility. In order to demonstrate MPA’s ability to optimize delays due to layer-2 authentication, we have experimented with three types of movement scenarios involving both roaming and non-roaming cases.

Mobility type	MIPv6				SIP Mobility	
	Buffering disabled, route optimization disabled	Buffering enabled, route optimization disabled	Buffering disabled, route optimization enabled	Buffering enabled, route optimization enabled	Buffering disabled	Buffering enabled
Handoff parameters						
L2 handoff (ms)	4.00	4.00	4.00	4.00	4.00	4.00
L3 handoff (ms)	1.00	1.00	1.00	1.00	1.00	1.00
Average packet loss	1.3	0	0.7	0	1.5	0
Average interpacket interval (ms)	16.00	16.00	16.00	16.00	16.00	16.00
Average interpacket arrival time during handover (ms)	21	45	21	67	21	29.00
Average packet jitter (ms)	n/a	29	n/a	51	n/a	13.00
Buffering period (ms)	n/a	50.00	n/a	50.00	n/a	20.00
Buffered packets	n/a	2.00	n/a	3.00	n/a	3.00

■ **Table 1.** Handoff performance of MPA-assisted MIPv6 and SIP-based mobility.

### MPA-ASSISTED LAYER 2 OPTIMIZATION

Currently, IEEE 802.11i cannot provide layer 2 pre-authentication during interdomain mobility. In order to demonstrate MPA's ability to optimize delays due to layer 2 authentication, we have experimented with three types of movement scenarios involving both roaming and non-roaming cases, as shown in Fig. 3. We have compared these results with the pre-authentication technique of IEEE 802.11i. In the roaming case the MN is visiting a domain that differs from its home domain. Consequently, the home AAA server needs to be contacted. For the non-roaming case, we assume the MN is moving between subnets within its visited domain, and only the local AAA server (AAAv) needs to be contacted. We have experimented with three scenarios.

The first scenario does not involve any pre-authentication. Because network layer authentication is not enabled and IEEE 802.11i pre-authentication is not used, the MN needs to engage in full EAP authentication with the target AP to gain access to the network after the move. The second scenario involves 802.11i pre-authentication. The third scenario takes advantage of MPA to provide layer 2 pre-authentication. In the testbed the MN moves between AP3 and AP4, which belong to two different domains where 802.11i pre-authentication is not possible. Diameter is used as the AAA protocol. In the roaming scenario the MN is initially connected to AP3 and starts PANA pre-authentication with the PANA authentication agent (PAA), which is collocated on the AR in the new candidate target network (R2 in network 2) from the current associated network (network 1). After authentication, the PAA installs a preshared key (PSK) in the target AP by using a preemptive key installation method. As the mobile moves to the target network, because PSK is already

installed, AP4 immediately starts the four-way handshake.

In our experiment, during the discovery phase, we assume that the MN is able to retrieve the IP address of the PAA and all required information about the Wi-Fi AP, such as channel and security-related parameters, at some point before handover. This avoids scanning during link layer handoff.

Table 2 shows the timing associated with some of the handoff operations we have measured during these operations.  $T_{auth}$  refers to the execution of EAP-TLS authentication [14];  $T_{conf}$  refers to the time spent during PSK generation and installation after EAP authentication is complete.  $T_{association} + 4way$  handshake refers to the time dedicated to the completion of association and the four-way handshake with the target AP after handoff. As demonstrated, MPA-assisted layer 2 pre-authentication provides comparable results with that of IEEE 802.11i, but also extends this functionality to interdomain mobility.

### MPA DEPLOYMENT ISSUES

In order to provide optimized handover for a mobile experiencing rapid subnet and domain changes, one needs to look into several operational issues. We describe some of the operational issues below.

#### DISCOVERY

The mobile can discover neighboring networks using mechanisms at several layers. CARD [7] helps discover candidate access routers in neighboring networks. The Service Location Protocol (SLP) [14] and Domain Name Service (DNS) can help provide addresses of the networking components for a given set of services in the specific domain. Pack *et al.* [15] provide a survey of layer-2-based fast handoff mechanisms to

Types of authentication	IEEE 802.11i EAP/TLS post-authentication		IEEE 802.11i pre-authentication		MPA-assisted layer 2 pre-authentication	
	Non-roaming	Roaming	Non-roaming	Roaming	Non-roaming	Roaming
Operation						
$T_{auth}$	61 ms	599 ms	98 ms	638 ms	177 ms	831 ms
$T_{conf}$	—	—	—	—	16 ms	17 ms
$T_{association}$ + four-way handshake	18 ms	17 ms	16 ms	17 ms	15 ms	17 ms
Total time	79 ms	616 ms	115 ms	654 ms	209 ms	865 ms
Time affecting handoff	79 ms	616 ms	16 ms	17 ms	15 ms	17 ms

■ **Table 2.** MPA-assisted layer 2 pre-authentication.

reduce the discovery related delay. 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 neighboring networks using information contained in the link layer. However, if the link layer management frames are encrypted by some security mechanism such as IEEE 802.11w, the MN may not be able to obtain the required information before establishing link layer connectivity to the access point. In addition, including this upper layer information may add to the burden of the bandwidth constrained wireless medium. When bandwidth is not a problem, a large beacon interval will introduce a long scanning time, resulting in interruptions. For these reasons, a higher-layer discovery protocol has advantages in obtaining the information regarding neighboring elements. The emerging IEEE 802.21 standard helps obtain this information about neighboring networks from an information server (IS). When the mobile's movement is imminent, it starts the discovery process by querying the IS and obtains the required parameters such as the IP address of the access point, its characteristics, routers, SIP servers, or authentication servers of the neighboring networks.

### MOBILITY RATE

It is important that handoff operations such as pre-authentication, secured tunnel establishment, and proactive binding update are completed successfully before the mobile is subjected to another handover. When a mobile is subjected to continuous handover, the inter-handoff interval of the mobile should not be faster than the MPA related pre-handover signaling latency. It is also important that the MN has the time budget to perform all these operations. For MPA to operate successfully at a higher movement rate, it is important to reduce pre-handover signaling latency. This can be achieved by executing handover keying re-authentication [16] over pre-authentication transport during the MPA pre-authentication phase. Alternatively, some

parts of the MPA operations (e.g., pre-authentication) can be performed before the handover and some parts (e.g., IP address acquisition and binding update) after the handover.

### TUNNEL MANAGEMENT

After an IP address has been proactively acquired from the DHCP server in a CTN, a proactive handover tunnel is established between the MN and the AR in the CTN. The MN uses the acquired IP address of the next network as the tunnel's inner address. In order for traffic to be directed to the MN after the MN attaches to the target network, the proactive handover tunnel needs to be deleted or disabled using a tunnel management protocol. Several protocols can be used for the tunnel management protocol. When IKEv2 is used for proactive IP address acquisition, it can also be used as the tunnel management protocol. Alternatively, PANA or a General Internet Signaling Transport (GIST)-based [17] application may be used as the secure tunnel management protocol. A link layer event such as SNR can trigger the tunnel management protocol.

### SECURITY ASSOCIATION MANAGEMENT

In the case of pre-authentication with multiple target networks, it is useful to maintain the state in the authentication agent of each of the neighboring networks for a certain time. Since an MN often moves back and forth between a small set of networks, networks and MNs should cache authentication state to accelerate establishing SAs when an MN returns to the current network. Thus, if the mobile does move back and forth between neighboring networks, already maintained authentication state can be helpful. When an MN that has been authenticated and authorized by an authentication agent in the current serving network makes a handover to a target network, it may want to hold the SA that has been established between the MN and the authentication agent for a certain time period so that it does not have to go through the entire authentication signaling process to create an SA from scratch if it returns to the previous network.

After an IP address has been proactively acquired from the DHCP server in a CTN, a proactive handover tunnel is established between the mobile node and the access router in the CTN. The mobile node uses the acquired IP address of the next network as the tunnel's inner address.

Supporting secured seamless handover over heterogeneous access networks involving inter-domain mobility needs to take into account access authentication and security association between the authentication agents in the neighboring networks.

## CONCLUSIONS

Supporting secured seamless handover over heterogeneous access networks involving interdomain mobility needs to take into account access authentication and security association between the authentication agents in neighboring networks. We provide an overview of media-independent pre-authentication and demonstrate that it can take care of the drawbacks associated with the existing mobility optimization techniques and support secured, optimized interdomain mobility. Our experimental results demonstrate that MPA can dramatically reduce interdomain handover delays independent of the type of access mechanism and mobility protocol. In particular, we experimented with 802.11 and CDMA access networks using both MIPv6 and SIP-based network layer mobility protocols. MPA can provide layer 2 security optimization during interdomain handover that is not possible by existing mechanisms, such as IEEE 802.11i.

## REFERENCES

- [1] A. Dutta *et al.*, "Experimental Analysis of Multi Interface Mobility Management with SIP and MIP," *IEEE Conf. Wireless Networks, Commun., and Mobile Comp.*, vol. 2, Maui, HI, June 2005.
- [2] B. Aboba and D. Simon, "PPP EAP TLS Authentication Protocol," IETF RFC 2716, Oct. 1999
- [3] T. Rückforth and J. Linder "AAA Context Transfer for Fast Authenticated Inter-Domain Handover," *Swisscom SA*, Mar. 2004.
- [4] H. Fathi, R. Prasad, and S. Chakraborty, "Mobility Management for VoIP in 3G Systems: Evaluation of Low-Latency Handoff Schemes," *IEEE Wireless Commun.*, vol. 12, no. 12, Apr. 2005.
- [5] K. El Malki, "Low-Latency Handoffs in Mobile IPv4," IETF RFC 4881, June 2007.
- [6] R. Koodli *et al.*, "Fast Handovers for Mobile IPv6," IETF RFC 4068, July 2005.
- [7] M. Liebsch *et al.*, "Candidate Access Router Discovery," IETF RFC 4066, July 2005.
- [8] J. Loughney *et al.*, "Context Transfer Protocol," IETF RFC 4067, July 2005.
- [9] H. Schulzrinne and E. Wedlund, "Application Layer Mobility Using SIP," *ACM MC2R*, vol. 4, July 2000.
- [10] D. B. Johnson, C. E. Perkins, and J. Arkko, "Mobility Support in IPv6," IETF RFC 3775, June 2004.
- [11] P. Calhoun *et al.*, "Diameter Base Protocol," IETF RFC 3588, Sept. 2003.
- [12] IEEE P802.21/D08.00, "Draft IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services," Jan. 2008.
- [13] D. Forsberg *et al.*, "Protocol for Carrying Authentication for Network Access," IETF draft, Sept. 2007, work in progress.
- [14] E. Guttman, C. Perkins, and J. Veizades, "Service Location Protocol," IETF RFC 2608, June 1999.
- [15] S. Pack *et al.*, "Fast Handoff Support in IEEE 802.11 Wireless Networks," *IEEE Commun. Surveys and Tutorials*, vol. 9, no. 1, 2007.
- [16] V. Narayan and L. Dondeti, "EAP Extensions for EAP Re-Authentication Protocol," draft-ietf-hokey-erx-08, Nov. 2007, work in progress.
- [17] H. Schulzrinne and R. Hancock, "GIST: General Internet Signaling Transport," draft-ietf-nsis-ntlp-15, Feb 2008, work in progress.

## BIOGRAPHIES

ASHUTOSH DUTTA [SM] (adutta@research.telcordia.com) is currently a senior scientist in Telcordia Technology's Inter-

net Network Research Laboratory. Prior to joining Telcordia Technologies, he was the director of Central Research Facilities at Columbia University from 1989 to 1997 and a computer engineer with TATAs from 1985 to 1987. His research interests include session control protocols and mobile wireless Internet. Ashutosh has a B.S. in electrical engineering (1985), an M.S. in computer science (1989), and is currently a part-time Ph.D. candidate at Columbia University. He currently serves as Chair of the IEEE Princeton and Central Jersey section. He is a senior member of the ACM.

DAVID FAMOLARI is a senior scientist and program manager within the Applied Research Department of Telcordia Technologies. He currently manages operations for a joint research collaboration, called ITSUMO, between Telcordia and Toshiba America Research Inc (TARI) that is delivering innovative mobility, QoS, configuration, and security technologies for the next generation of wireless IP networks. He holds B.S. and M.S. degrees in electrical engineering from Rutgers University, and has completed Ph.D. coursework at Columbia University.

SUBIR DAS is a senior scientist in the Mobile Networking Research Department of Telcordia Technologies Inc. since 1999. From 1997 to 1999 he was a faculty member in the E&ECE Department, Indian Institute of Technology, Kharapur. He has published more than 50 papers in the area of wireless networking. He has four U.S. patent to his credit and more than a dozen applications pending. His current research interests include IP mobility management and optimization, next-generation all-IP network architecture and protocols, security in wireless IP networks, IP multimedia subsystems, and fixed-mobile convergence.

YOSHIHIRO OHBA is a research director at Toshiba America Research Inc. He received B.E., M.E., and Ph.D. degrees in information and computer sciences from Osaka University in 1989, 1991, and 1994, respectively. His interest is standardizing security and mobility protocols. He is chair of the Security Study Group in the IEEE 802.21 Working Group.

VICTOR FAJARDO is a researcher at Toshiba America Research Inc. He received his M.S. in computer science and B.S. in electrical engineering from California Polytechnic University, Pomona. He is currently working on network mobility and security. Prior to this he worked on traffic engineering for core network platforms.

KENICHI TANIUCHI (kenichi.taniuchi@toshiba.co.jp) is a research scientist at the Communication Platform Laboratory, Toshiba R&D Center, Japan. He received his B.S. and M.S. degrees from Waseda University, Tokyo, Japan, in 1998 and 2000, respectively. Since joining Toshiba in 2000 he has worked on research and development for ad hoc networks. From 2003 to 2007 he worked on the ITSUMO project at Toshiba America Research, Inc and worked with Telcordia on research in mobility and security with standardization of IEEE 802.21.

RAFAEL MARIN LOPEZ is a full-time assistant lecturer in the Department of Information and Communications Engineering at the University of Murcia (Spain). He has collaborated in several European research projects and spent a year with Toshiba America Research, Inc. (TARI). Additionally, he collaborates actively in IETF, above all in the PANA and HOKEY WGs. His main research interests include network access authentication and security in mobile networks.

HENNING SCHULZRINNE [F] (hgs@cs.columbia.edu.) is a professor in the Department of Electrical Engineering and chair of the Department of Computer Science at Columbia University, New York. He has a Ph.D. from the University of Massachusetts; worked at Bell Laboratories, Murray Hill, and GMD Fokus, Berlin. His research interests include Internet multimedia and telephony services, signaling, network quality of service, scheduling, multicast, performance evaluation. He is a co-author of the Internet standards track protocols RTP, RTSP, SIP, and GIST.