Wireless Pers Commun
DOI 10.1007/s11277-007-9266-3

Seamless proactive handover across heterogeneous access networks

Ashutosh Dutta · Subir Das · David Famolari · Yoshihiro Ohba · Kenichi Taniuchi · Victor Fajardo · Rafa Marin Lopez · Toshikazu Kodama · Henning Schulzrinne

Received: 22 May 2006 / Accepted: 22 January 2007

Abstract Dual-mode handsets and multimode terminals are generating demand for solutions that enable convergence and seamless handover across heterogeneous access networks. The IEEE 802.21 working group is creating a framework that defines a Media Independent Handover Function (MIHF), facilitates handover across heterogeneous access networks and helps mobile users experience better performance during mobility events. In this paper, we describe this 802.21 framework and also summarize a Media-independent Pre-Authentication (MPA) mechanism currently under discussion within the IRTF that can further optimize handover performance. We discuss how the 802.21 framework and the MPA technique can be integrated to improve handover performance. Finally, we describe a test-bed implementation and validate experimental performance results of the combined mobility technique.

A. Dutta (✉) · S. Das · D. Famolari
Mobile Networking Research, Telcordia Technologies, 1 Telcordia Drive, RRC - 1A220, Piscataway, NJ, 08854, USA
e-mail:adutta@research.telcordia.com

Y. Ohba · K. Taniuchi · V. Fajardo · R. M. Lopez · T. Kodama
Toshiba America Research Inc., P.O. Box 429, Piscataway, NJ 08854, USA

H. Schulzrinne
Computer Science Department, Columbia University, New York, NY, USA

Keywords IEEE802.21 · Heterogeneous handover · Seamless mobility · Media independent pre-authentication

1 Introduction

Future network devices will need to roam seamlessly across heterogeneous access technologies such as 802.11, WiMAX, CDMA, and GSM, between wired networks such as xDSL and cable, as well as between packet switched and circuit switched (PSTN) networks. Figure 1 shows an example wireless Internet roaming scenario across heterogeneous access networks that involves intra-subnet, inter-subnet, and inter-domain mobility. Supporting seamless roaming between heterogeneous networks is a challenging task since each access network may have different mobility, QoS and security requirements. Moreover, interactive applications such as VoIP and streaming media have stringent performance requirements on end-to-end delay and packet loss. The handover process stresses these performance bounds by introducing delays due to discovery, configuration, authentication and binding update procedures associated with a mobility event.

The overall handover delay can be attributed to operational delays at all layers of the protocol stack including layer 2, layer 3 and the application layer. Performance can also be tied to the

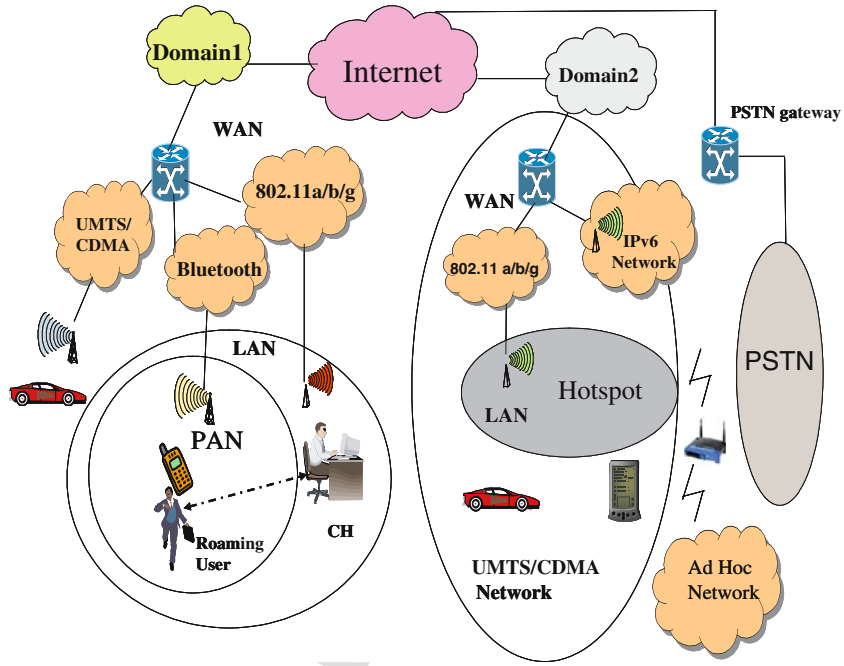

Fig. 1 Wireless internet roaming scenario

specific access networks and protocols that are used for network access. For example, configuring a PPP (Point-to-Point Protocol) interface in a WAN environment takes more time than configuring an interface using DHCP (Dynamic Host Configuration Protocol) in a LAN environment. Access network-specific authentication and authorization protocols may introduce additional delays. It is observed that traditional non-optimized handover takes up to 4 s delay during inter-LAN movement. Thus in a typical deployment scenario, several hundred (~200–300) packets may be lost during the handover. Also, it may take up to 15 s to complete authentication and connection establishment procedures if the neighboring network is either CDMA or GPRS. Movement between two different administrative domains poses additional challenges since a mobile will need to re-establish authentication and authorization in the new domain. Layer 2 handoff delay is more relevant when an authentication process is involved to obtain layer 2 connectivity. Experimental studies [1,21] with network handovers indicate that the latency introduced due to scanning and authentication at layer 2 is not acceptable for real time communications. For example, in IEEE 802.11 based wireless networks, the IEEE 802.11i security mechanism performs a new set of exchanges with the authenticator in the target AP in order to initiate an EAP (Extensible Authentication Protocol) exchange to an authentication server. Following a successful authentication, a 4-way handshake with the wireless station derives a new set of session keys for use in data communications. This process can significantly prolong the handover event and calls for improved latency performance in layer 2 security mechanisms related to handover.

In order to provide an improved, secured mobility management solution for real-time communication involving heterogeneous handover, we have designed an optimization scheme that takes advantage of IEEE 802.21 [14] services and a new technique called Media independent Pre-Authentication (MPA) [8]. MPA enables mobile devices to expedite layer 2 pre-authentication in the neighboring network, to proactively obtain an IP address, and to perform mobility related binding updates ahead of the anticipated handover. MPA also helps to bootstrap layer 2 security in the target network while the mobile is still connected in the current network. MPA thus provides an access independent pre-authentication mechanism that does not require support for different layer 2 authentication and encryption mechanisms.

The rest of the paper is organized as follows. Related work in mobility optimization is described in Sect 2. Section 3 describes the IEEE 802.21 framework, its core architecture and the functional components. An example of MPA assisted 802.21-based mobility is illustrated in Sect. 4. Results of a test-bed implementation involving the 802.21 Information Service (IS), Event Service (ES), and MPA framework for two different types of handover scenarios are described in Sect. 5. Section 6 highlights certain features of MPA that are different than existing make-before-break mechanisms and FMIPv6. Finally, Sect. 7 concludes the paper.

2 Related work

References [6,11,17,18,20,26,32,36] describe mobility management techniques that support fast-handover by enhancing currently available mobility management protocols for both IPv4 and IPv6. Reference [32] attempts to reduce delay at layer 2 by reducing the scanning time, whereas refs. [6,26] devise mechanisms to reduce handover delay at layer 3 and application layer respectively. Similarly refs. [3,33] try to reduce the layer 2 authentication delay during handover. NETLMM working group within the IETF is working defining a design team document [18] that aims at reducing the delay during intra-domain handoff. There is also relevant work undertaken by various standards organizations. IEEE 802.11i defines a pre-authentication mechanism for use in 802.11 variant wireless networks. This mechanism allows mobile devices to pre-authenticate by establishing link-layer security associations with one or more target authenticators by sending 802.1X messages directly to the target authenticators bridged via the serving authenticator. IEEE 802.11f has defined transfer of security context from one AP to another. Presently, IEEE 802.11r Task Group has been working to define fast BSS transition mechanisms involving a definition of key management hierarchy and mechanisms for link-layer pre-authentication and setup of session keys before the re-association to the target AP. These mechanisms are defined for 802.11 technologies only and are only applicable within an access domain [e.g., same ESS (Extended Service Set)] and do not support inter-ESS or inter-domain handover within 802.11 access technology.

Currently, there are several initiatives to optimize mobility across heterogeneous networks. The MOBOPTS working group within the IRTF (Internet Research Task Force) and the DNA (Detecting Network Attachment) working group within the IETF have been investigating ways to support optimized handover by using appropriate triggers and events from the lower layers. References [4,7] describe mobility management techniques that consider both security and heterogeneous mobility. Although many of these techniques use cross-layer mechanisms and "make-before-break" algorithms to provide fast-handover, it is desirable to have a standardized method to handle mobility across heterogeneous networks in an efficient manner. The IEEE 802.21 [14] working group is currently working towards a Media Independent Handover framework and is creating a standard that facilitates handover in a heterogeneous access environments. This framework provides assistance to underlying mobility management approaches by allowing information about neighboring networks, link specific events and commands that are necessary during handover process to be exchanged between 802.21 entities. MPA [8] is being discussed within the IRTF as a way to further improve service quality and user experience during handover events. In this paper, we discuss how MPA and 802.21 can be used together to improve handover performance in heterogeneous access networks. We describe how the two approaches can be integrated and present experimental results obtained on a prototype test-bed implementing the 802.21 and MPA concepts. We also describe how MPA can reduce layer 2 handover delay by bootstrapping layer 2 pre-authentication in the previous network. Lastly, we provide a brief comparison with the existing fast-handover technique FMIPv6 [4].

3 IEEE 802.21 framework

The IEEE 802.21 framework is intended to facilitate handover between heterogeneous access networks by exchanging information and defining commands and event triggers to assist in the handover decision making process. The framework

within 802.21 helps mobile devices to discover, characterize, and select networks within their current neighborhoods by exchanging information about available link types, link identifiers, and link qualities of nearby network links. This process of network discovery and selection allows a mobile to connect to the most appropriate network based on certain mobile policies.

The heart of the 802.21 framework is the Media Independent Handover Function (MIHF) which provides abstracted services to higher layers by means of a unified interface. This unified interface exposes service primitives that are independent of the access technology. The MIHF can communicate with access specific lower layer MAC and PHY components, including those of 802.16, 802.11 and cellular, as well as with upper layer entities. The MIHF and its relationship with upper and lower layer elements are shown in Fig. 2. MIHF defines three different services: Media Independent Event Service (MIES), Media Independent Command Service (MICS) and Media Independent Information Service (MIIS). In the following subsections, we describe these three main functional components in greater detail.

3.1 Media Independent Event Service

Media Independent Event Service (MIES) provides services to the upper layers by reporting both local and remote events. Local events take place within the local stack of the mobile node, whereas remote events take place in another MIHF in the network. The event model works according to a subscription and notification procedure. An MIH user (typically upper layer protocols) registers to the lower layers for a certain set of events and gets notified as those events take place. In the case of local events, information propagates upward from the lower layer to the MIH layer and then to the upper layers. In the case of remote events, information may propagate from the MIH or Layer 3 Mobility Protocol (L3MP) in one stack to the MIH or L3MP in a remote stack. Some of the common events defined include "Link Up," "Link Down," "Link Parameters Change," "Link Going Down," "Handover Imminent," etc. As the upper layer gets notified about certain events it makes use of the command service to control the links to switch over to a new point of attachment.

3.2 Media Independent Command Service

The higher layers use the (Media Independent Command Services) MICS primitives to control the functions of the lower layers. MICS commands are used to gather information about the status of the connected links, as well as to execute higher layer mobility and connectivity decisions to the lower layers. MIH commands can be both local and remote. These include commands from the upper layers to the MIH and from the MIH to the lower layers. Some examples of MICS commands are MIH Poll, MIH Scan, MIH Configure, and MIH Switch. The commands instruct an MIH device to poll connected links to learn their most recent status, to scan for newly discovered links, to configure new links and to switch between available links.

3.3 Media Independent Information Service

Mobiles on the move need to discover available neighboring networks and communicate with the elements within these networks to optimize the handover. The MIIS defines information elements and corresponding query-response mechanisms that allow an MIHF entity to discover and obtain information relating to nearby networks. The MIIS provides access to information, including network type, roaming partners, service providers of the neighboring networks, channel information, MAC addresses, security information, and other information about higher layer services helpful to handover decisions. This information can be made available via both lower and upper layers. In some cases certain layer 2 information may not be available or sufficient to make intelligent handover decisions. In such scenarios, higher-layer services may be consulted to assist in the mobility decision-making process.

The MIIS specifies a common way of representing information by using standard formats such as XML (eXternal Markup Language) and TLV (Type-Length-Value). Having a higher layer

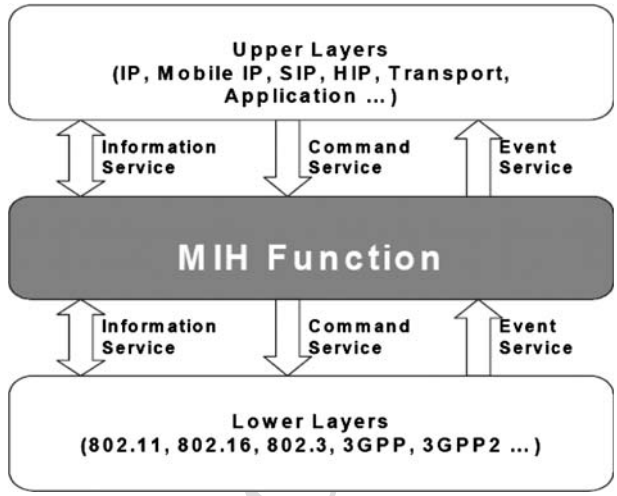

Fig. 2 Media independent handover function location and key services (Source: IEEE D01)

mechanism obtain information about neighboring networks of different access technologies alleviates the need for a specific access-dependent discovery method. We have implemented an MIIS based on the Resource Description Framework (RDF) [29] and XML as part of our prototype.

4 Mobility optimization using 802.21 and MPA

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 (CTN), but is also able to send and receive IP packets using the obtained CTN IP address before it physically attaches to the CTN. This ability to communicate at layer-3 before establishing layer-2 connectivity is a great benefit in terms of reducing handover delays.

The MPA procedure works as follows. An MPA mobile device first establishes a security association with a CTN via its existing network connection using the Protocol for carrying Authentication and Network Access (PANA) [24] to obtain configuration information that will allow it to participate in the new network. Next, a bi-directional tunnel is established between the device and the Access Router (AR) of the CTN. IP packets can be sent over this tunnel. At this point, all the necessary layer 3 mechanisms have been completed to enable handover, however the device has not yet established layer 2 connectivity with the CTN. Once this has been established, the bi-directional tunnel can be removed and the handover is complete. By pre-authenticating, pre-configuring the link and establishing a secure tunnel, the handover can complete with reduced delays and fewer lost packets.

MPA however, does not perform network discovery and relies on outside mechanisms to discover CTNs. In this sense, MPA and 802.21 can be very complementary to each other with 802.21 providing network discovery and making available information to assist in mobility decisions. MPA can ensure that the security associations are in place and that devices can authenticate with candidate networks before mobility decisions are executed. These security associations can happen at different layers of the protocol stack.

The service primitives defined in the 802.21 framework can work with any type of layer 3 and above mobility management protocol such as SIP [31], MIPv6 [16] or MIPv4 [27]. A mobile uses the service primitives to communicate with policy managers, device drivers and other mobility management protocols during its movement.

Figure 3 shows an illustration of how MPA and 802.21 can work in conjunction with a SIP-based mobility management mechanism. As shown, the mobile has two types of interfaces [Network X (e.g., 802.11) and Network Y (e.g., CDMA)]. Initially, the mobile is using Network X as its primary interface to establish a multimedia session

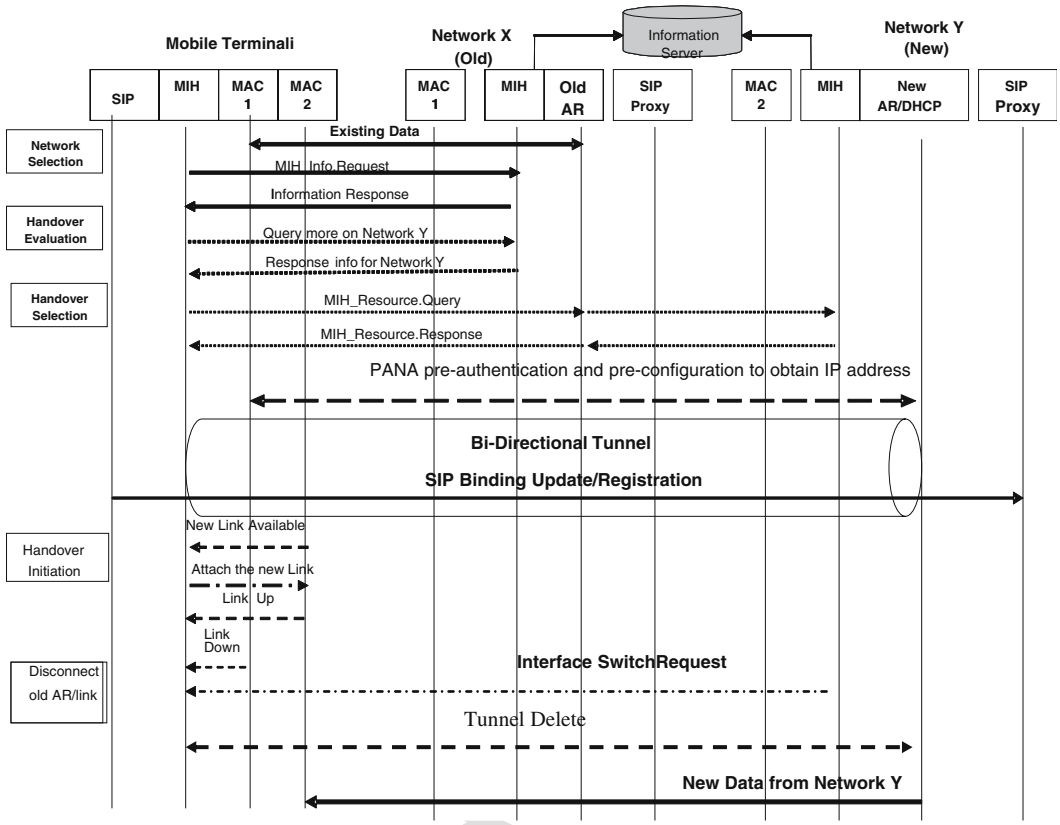

Fig. 3 802.21 assisted SIP-based mobility management for heterogeneous handover

with a correspondent host. The mobile queries an information server to learn about available networks that are of type Y. The mobile makes an MIH query to verify that the required resources to sustain the session are available. It then selects an appropriate network and retrieves more information about that network, such as the address and the type of security servers, DHCP server address, MAC address of the access point, etc. With this information, the mobile initiates MPA procedures to pre-authenticate with network Y and configures itself for operation in that network. These operations could include layer 3 pre-configuration, layer-2 pre-authentication by pre-establishing the keys in the neighboring access points, proactive binding update (e.g., SIP ReINVITE), etc. At this point the mobile is ready to switch layer-2 connections when appropriate by using IEEE 802.21 command primitives such as "Initiate Handover." Once the "Link up" event is received from the MIES indicating that the target layer 2 connection is ready, the mobile starts using the new interface. The "Link down" command can delete the proactive tunnel. At this time, traffic to the mobile flows through the new interface and the handover is complete. In the case of handover involving single interface the sequence of events will take a different order, since the same physical interface participates in communication both before and after the handover. The physical interface gets configured with two logical addresses, one from the current network and one from the next network during the handover process.

5 Implementation and experimental results

This section describes an implementation based on the 802.21 framework and MPA scheme, and provides performance results and compares these with non-optimized mobility management. Figure 4a shows the experimental test-bed with four networks

defined. We have experimented with two kinds of handover scenarios: one between two 802.11 networks belonging to different administrative domains; the other between 802.11 and CDMA1x-EVDO access networks. For both the cases, we demonstrate how the 802.21 information discovery, event service and MPA framework help to improve performance during handover. Case I deals with terminals equipped with a single 802.11 interface, and case II deals with terminals with two different types of interfaces. The event services Link Up and Link Down act as triggers to help the handover. We apply Link Up event notification for the handover involving 802.11 access networks, and we apply Link Down event notification for the handover involving EVDO and 802.11 networks. However, events such as Link Going Down and Link Going Up maybe more appropriate for dual-mode devices. Figure 4b, c illustrate the mechanism associated with both of these cases, respectively. Additionally, we also describe experimental results of MPA-assisted layer 2 pre-authentication applied to intra-technology and inter-domain handovers in Sect. 5.3. We describe the details in the following sections.

5.1 Intra-technology, inter-domain handoff

In Figure 4a, Network 1 is the current point of attachment (cPoA), Networks 2 and 3 are possible new points of attachment (nPoA), and network 4 is where the correspondent node (CN) resides. The mobile is initially in Network 1 and starts communicating with the correspondent node.

Media-independent Pre-Authentication is independent of the underlying mobility management protocol and we have demonstrated MPA using both SIP Mobility (SIP-M) [31] and MIPv6 [16] as mobility management protocols. The configuration protocol is DHCP, the authentication agent (AA) is a PANA [24] server with a backend Diameter server to carry out EAP-TLS (Extensible Authentication Protocol) [1]. The configuration agent (CA) is a DHCP Relay Agent and the Next Access Router (NAR) is an edge router running the Linux operating system. We have used IP-IP tunneling functions for SIP-based mobility and have taken advantage of IPSEC tunnel for MIPv6. After a successful connection setup using SIP, voice traffic flows between the MN and the CN. This voice traffic is carried over RTP/UDP. We have

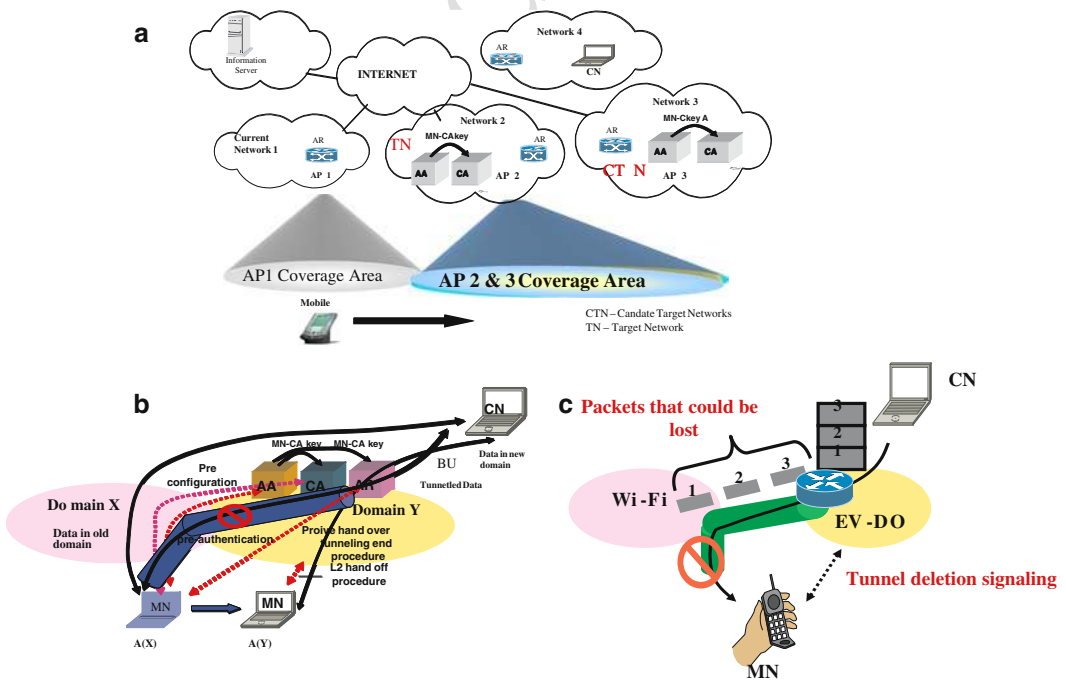

Fig. 4 Experimental setup for MPA and 802.21 assisted handover. (**a**) Logical test bed scenaria, (**b**) Intra-technology. Inter-domain, (**c**) Inter-technology, Inter-domain

used RAT (Robust Audio Tool) as the media agent and the streaming traffic is generated using a codec with a spacing of 20 ms between packets.

For non-optimized handovers (those that do not employ 802.21 and MPA mechanisms, the handover delay and packet loss take place during the mobile's layer 2 movement, IP address assignment, post-authentication, and mobility binding update. The DHCP interaction takes a long time to complete the detection of duplicate IP addresses and the binding updates can be delayed if the correspondent node is too far from the mobile node. The experimental results show that 4 s of delay are attributed to the above factors. We observed approximately 200 packets were lost due to this delay. The situation is worse in case II, where it may take up to 15 s to authenticate and establish connectivity with CDMA network.

These delays can be reduced by taking advantage of the network discovery mechanisms of 802.21 and the pre-authentication technique of MPA. The 802.21 framework provides details of neighboring networks that may include channel numbers, addresses of APs, DHCP servers, PANA servers, etc. Such information helps the mobile communicate with network elements ahead of time and perform a proactive handover. We have used an RDF/XML-based query and response mechanisms to obtain the required information from the information server. We briefly describe the related software modules that were used to obtain the relevant neighborhood information from the information server. Details of the mechanism including the RDF schema can be found in reference [10]. In our testbed, at the information server we use Joseki to interpret the RDQL [29] and send appropriate responses to the client. We use Jena [15], which is a Java framework for building semantic Web applications, for forming RDQL. It provides a programmatic environment for RDF, RDFS and OWL, including a rule-based inference engine.

We have used the Joseki server for publishing RDF models on the web. These models are represented by URLs and can be accessed by query using HTTP GET. These queries and responses can also be implemented using the Media Independent Handover protocol currently being defined by IEEE 802.21 working group. We implemented HTTP as the transport since the MIH protocol transport mechanisms were not complete at the time of experimentation.

We provide sample results of queries and responses and timing break downs for some typical queries in Table 1. The queries shown in Table 1 can primarily be divided into meta queries and secondary queries. A meta query provides general information about the neighboring networks, while a secondary query provides detailed information about that network's elements. Query–response times can vary depending upon the network access delays and processing times. For example, API delay represents the delay incurred during interaction with the query application at the mobile and server. Processing delay at the client and server includes the time spent for HTTP processing. Network delay is the delay to transmit the TCP packets between the mobile and server. However, since these queries are carried out prior to the handover event, they do not contribute to handover delay and also do not result in packet loss. Successful handovers require that the information query and response are completed before the layer-2 handover, therefore these query and response delays are critical. We ran experiments with Mobile IPv6, with and without Route Optimization (RO), as well as with SIP as the underlying mobility management protocol. In addition, we also examined the effects of buffering at the edge router that helps to reduce the packet loss during handover.

Figure 5a compares the results of the audio output with the non-proactive scheme, where as Fig. 5b shows several handoff statistics such as packet loss, delay, and jitter values with and without buffering mechanism. Handover delays are dramatically reduced from those reported earlier; reducing the time from seconds to milliseconds. Proactive discovery of the target AP also helped reduce the layer 2 delay since it avoided scanning and the EAP-TLS procedure needed for full EAP authentication. Details of layer 2 pre-authentication are described in Sect. 5.3. Packet losses were also reduced due to handoff optimization at all layers. As expected, no packets were lost with buffering enabled. The Dynamic buffering scheme on the edge router helps to maintain a tradeoff between the packet loss and additional delay. The highlighted numbers show that we were able to achieve zero packet loss while keeping the delay between last

Table 1 Sample query response for 802.21 MIIS

Query	Response	Processing delay (ms)	
Current PoA: *AP,*	Neighbor 0 PoA: ID:00:20:A6:53:B2:5E, Tariff: 20	Total	2,292
Query: *Provide list of 802.11-type neighboring networks and their with associated tariff values*	Neighbor 1 PoA : ID:01:23:45:67:89:AB, Tariff:50	API	1,291
		Network	919
		Server	18
		Client	64
Neighbor 0 selected	Target network channel: 10 SSID: ITSUMO newpoa1	Total	1,473
Query: *Provide list of network elements for Neighbor 0*	Router address: 10.10.10.52	API	991
	Router MACID: 00:00:39:e6:8b:ee	Network	451
	Subnet: 255.255.255.0	Server	13
	DHCP Server: 10.10.10.52	Client	18

pre-handoff packet and first in-handoff packet to a value within the threshold limit during the handover.

It is worthwhile to discuss the techniques that were used to optimize the layer 2 handoff delay in the experiment. In general, 802.11 layer 2 handoff delay consists of many phases such as scanning, association, and authentication. In general, as the SNR (Signal-to-Noise Radio) of the mobile with the current AP goes below certain threshold, the mobile starts the scanning procedure by issuing a MLME-SCAN.request primitive [2] to discover the characteristics of the neighboring APs. Reference [21] shows that scanning (discovery phase) takes the maximum amount of time during layer 2 handover, since the mobile needs to scan all the channels before associating with a specific channel. There are related works [7] that reduce the layer 2 scanning time by using different scanning algorithms. In this proposed scheme, network discovery and selection are done proactively. By using IEEE 802.21 information discovery service and the current location of the mobile node, we can obtain information such as the channel number and ESSID of the access point in the neighboring networks which are needed by MLME-ASSOCIATE.request primitive. Based on this knowledge, the mobile can associate with the desired channel number in the target network directly without performing the regular channel scanning operation. As a consequence, it is not required that target APs operate in the same channel. This mechanism is useful independent of whether the target AP is working on the same channel or has the same ESSID as the current one. Since the mobile knows the AP's channel number and ESSID it can change channel and engage the target AP without incurring the delays associated with scanning. To realize this capability, we modified the IEEE 802.11 MADWIFI driver [22] on the mobile device to use the neighboring access point information from the IEEE 802.21 information service and to issue "Association Request" commands to connect to neighboring APs. This modification eliminates the need for the regular channel scanning procedure during handover.

5.2 Inter-technology, inter-domain handoff

Handover involving heterogeneous access can take place in many different ways depending upon the activity of the second interface. In one scenario, the second interface comes up when the link to the first interface goes down. This scenario usually gives rise to undesirable packet loss and handoff

a

Non-802.21 assisted SIP-based mobility

802.21 assisted SIP-based mobility – Optimized handoff

b

Mobility Type	MIPv6				SIP Mobility	
Hand off Parameters	Buffering Disabled + RO Disabled	Buffering Enabled + RO Disabled	Buffering Disabled + RO Enabled	Buffering Enabled + RO Enabled	Buffering Disabled	Buffering Enabled
L2 hand off (ms)	4.00	4.33	4.00	4.00	4.00	5.00
Avg. packet loss	1.33	0	0.66	0	1.50	0
Avg. inter-packet interval (ms)	16.00	16.00	16.00	16.00	16.00	16.00
Avg. inter-packet arrival time during handover (ms)	n/a	45.33	n/a	66.60	n/a	29.00
Avg. packet jitter (ms)	n/a	29.33	n/a	50.60	n/a	13.00
Buffering period (ms)	n/a	50.00	n/a	50.00	n/a	20.00
Avg. Buffered Packets	n/a	2.00	n/a	3.00	n/a	3.00

Fig. 5 (**a**) Recorded signal activity: Non-optimized versus optimized. (**b**) Delay and packet loss statistics optimized

delay. In a second scenario, the second interface is prepared proactively while the mobile still communicates using the first interface, and at some point the mobile decides to use the second interface as the active interface. This results in less packet loss as it uses make-before-break techniques. In the third scenario, all the required state and security associations (e.g., PPP state, LCP, CHAP in case of CDMA networks) are established ahead of time thus reducing the time taken for the secondary interface to be attached to the network. This third scenario may be beneficial from a battery management standpoint. Devices that operate two interfaces simultaneously can rapidly deplete their batteries otherwise. However, by activating the second interface only after an appropriate network has been selected battery power may be used more efficiently. This third scenario demonstrates the usefulness of 802.21's Event Service (ES), Information Service (IS) and MPA.

Information discovery and MPA remain the same as in Sect. 5.1 with intra-technology handover. In this experiment we also add a faster link down detection mechanism and a copy-forwarding technique at the access router to help reduce transient packet loss during handover. We briefly discuss these two procedures. The fast link down detection method is used to provide fast "link down"

event indication and helps in quickly assisting layer-3 protocols to take necessary actions. The quick "link down" event indication uses a combined scheme of passive monitoring of 802.11 frames as well as active probing of the AP at certain conditions. A quick indication can provide better handoff performance to L3 handoff procedures. The copy forwarding scheme takes advantage of the buffering in the edge routers, in addition, it also forwards the duplicate packets that it buffers. An MN that requests the copy-forward service from the (Current Point of Attachment) network will signal the CPFW (Copy-and-Forward) node of its intent to use the said service prior to handoff. This signal is referred to as a copy request. Upon receiving the request, the CPFW node will start to classify and copy packets destined for the MN on the CPA. This process does not stop the original packets from being forwarded to the MN in the CPA. The limit for the amount of packets copied will be based on the estimated time it takes for the MN to complete the handover. As a result the mobile may end up getting duplicate packets, but packet loss is reduced. In this scenario, the mobile is initially communicating using its first interface over technology X (e.g., 802.11). It then uses 802.21 and MPA to discover a new access network of technology Y (e.g., CDMA), learn the addresses of configuration elements in that network, and then proactively prepare the required state information for its second interface to use technology Y. It then sets up proactive tunnels with the required access routers in the target network and establishes the security association. Next, the device uses Link Down event notification triggers to the upper layers to initiate the handover process to the newly available interface. Since most of the required events such as IP address acquisition, authentication, security association, and binding update have already been taken care of, the handover completes in less time.

We present results showing the usefulness of fast link detection, copy-forwarding and MPA in Fig. 6. Figure 6c shows the results of optimized handover that uses MPA and IEEE 802.21. As compared to non-optimized handover as shown in Fig. 6a and b that may result in delays up to 18 s and packet losses of 1,000 packets during handover from WLAN to CDMA, we were able to achieve zero packet loss, and 50 ms handoff delay between the last pre-handoff packet and first in-handoff packet. This handoff delay includes the time due to "link down detection" event and the time needed to delete the tunnel after the mobile has moved. Thus, the handoff delay in the experiment partly depends upon the RTT (Round Trip Time) in the CDMA network. However we observed about 10 duplicate packets because of the copy-forwarding mechanism at the access routers. These duplicate packets are usually handled easily by the upper layer application. These experimental results were taken using SIP-based mobility over IPv4 networks because of the unavailability of IPv6 deployment over the carrier's CDMA2000 network. But we expect similar results if these sets of experiments are carried out using MIPv6.

5.3 MPA-assisted layer 2 pre-authentication

In Sect. 5.1 and 5.2 we described how MPA in conjunction with 802.21 can help to optimize upper layer operations during heterogeneous handover. In this section, we describe how a combination of IEEE 802.21's information service and MPA can assist in reducing the layer 2 delay during inter-domain handover. Mishra et al. describe several components that contribute to the layer 2 handoff delay in Refs. [21,33]. References [3,12,32,33] describe mechanisms to reduce several components of layer 2 delay. The IEEE 802.11i pre-authentication provides a mechanism to optimize handover between APs by reducing the authentication process delay. Primarily, this mechanism consists of starting an EAP authentication with a target AP through the current associated AP. In fact, IEEE 802.11i specification provides the possibility to skip EAP authentication when there is a key (named PMK Pairwise Master Key), in the PMK Security Association cache or when Pre-Shared Key (PSK) mode is used. It is also important to mention that [33] provides a solution based on PMK pre-installation. The pre-installation is carried out by the MN's home AAA server. However this creates some deployment issues in roaming scenarios since visited domains may not always allow other domains to install cryptographic material in their own access points. In our approach, however, an entity in the visited domain

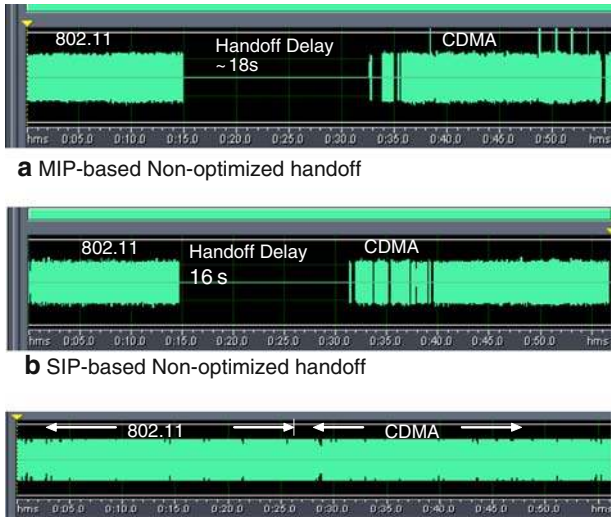

Fig. 6 Recorded signal activity MPA and IEEE 802.21 assisted handoff—Case II—Inter-technology, Inter-domain handoff. (**a**) MIP-based non-optimized handoff, (**b**) SIP-based non-optimized handoff. (**c**) MPA 802.21 assisted optimized handoff

a MIP-based Non-optimized handoff

b SIP-based Non-optimized handoff

c MPA and 802.21 assisted optimized handoff

(PAA) is in charge of doing this task without involving the home domain.

One important limitation of the IEEE 802.11i pre-authentication is the fact it can only work when APs are connected to the same distribution system (DS) and can exchange layer 2 frames. As a consequence, IEEE 802.11i pre-authentication between APs that belong to different administrative domains (inter-domain handoff) is not possible. Additionally, as another limitation, this mechanism involves a full EAP authentication with each candidate AP and thus the home AAA server is contacted every time the mobile moves. Thus, for the cases when IEEE 802.11i pre-authentication cannot be run, the MN has to run a full EAP authentication just after association with the new AP because it cannot be done through the current AP. This considerably increases the handover time as we have observed in our experiments. This limitation of 802.11i pre-authentication warrants an alternative solution to deal with layer 2 handoff where IEEE 802.11i pre-authentication cannot be applicable.

MPA in conjunction with 802.21 Information Service can help overcome the limitations associated with IEEE 802.11i pre-authentication.It does so by proactively installing the needed cryptographic material to create a security association at layer 2 that reduces the layer 2 handover delay and eventually the overall handoff time. We describe two experiments to illustrate the benefit of MPA-based layer 2 pre-authentication: non-MPA assisted handoff and MPA assisted handoff. We have considered IEEE 802.11 layer 2 technology as the candidate for this experiment although the MPA mechanism is access independent.

In the non-MPA case, the MN is initially attached to an open AP (current AP) and it moves to an IEEE 802.11i enabled AP in a new domain. As in the normal handover case, after disassociation with the open AP, the MN scans and discovers the target AP. After the association process, the MN needs to authenticate with the target AP by running a full EAP authentication. We have used EAP-TLS because it is a common authentication method and it has been used in other related works such as [12,33]. EAP-TLS authentication method is also used between MN and a backend authentication server.

In the second scenario, we have used MPA and 802.21-based information service. In this case, before the movement, the MN obtains the information about possible candidate target APs and also about the PANA Authentication Agent (PAA). Then, just after establishing a security association with the Candidate Target Network (CTN) via its current associated AP, the authentication agent (PANA server) derives a key for the mobile and

each possible candidate AP controlled by that PANA server. Each specific key is installed at each candidate target AP by using SNMPv3. Note that after PANA authentication, the MN is also able to derive the same keys for each candidate target AP that can potentially be used for running 802.11i 4-way handshake. Because PAA installs these keys and MN has the same keys, EAP does not need to be executed at the target APs after the MN moves. As the final step, the MN needs to associate with the selected candidate target AP and complete the needed 4-way handshake. Scanning operation during the discovery phase is avoided and EAP-TLS authentication is no longer needed to establish an 802.11i security association. Furthermore, when the MN moves between APs under the same PAA, the MN can just run the association and 4-way handshake procedures. It is important to note that the precise location of the mobile with respect to the target network access point ensures that the mobile is within the AP's reach before it associates with the AP without doing any scanning. IEEE 802.21 information service and single probe-request response message by the mobile can help achieve this. Fig. 7a, b illustrate the signal flows and the results of non-optimized L2 handoff and MPA-assisted optimized handoff, respectively.

As observed in Fig. 7b, scanning and EAP-TLS authentication operations are totally skipped during the MPA-assisted handoff. Scanning was avoided because 802.21-based Information Service provided the details of the access point and EAP-TLS was not necessary as the keys were distributed prior to the handoff. These two operations basically contribute to 97% of the overall layer 2 handoff delay in our experiments. Specified scanning times have been measured in an environment with many surrounding active APs operating at different channels. As per [21] it leads to higher scanning time because there are active APs in each scanned channel and the mobile spends more time waiting for probe responses in every channel. Additionally, the AAA server is placed only two hops away from the APs and certification validation is performed locally. As a consequence, the time taken for EAP-TLS (~94 ms) may be shorter than in other network architectures, Note that typically the AAA server is placed far from APs and some kind of additional certificate validation steps are normally carried out increasing the overall EAP-TLS authentication process. In fact, as other experimental results [12,33] show, an EAP-TLS can cost even seconds (1.1 s and 5.1 s, respectively). These times are unacceptable for suitable handoff performance. As evident from Fig. 7a and b, the MPA-based solution reduces the layer 2 handoff delay to only three main factors: authentication, association and 4-way handshake time. MPA can achieve layer

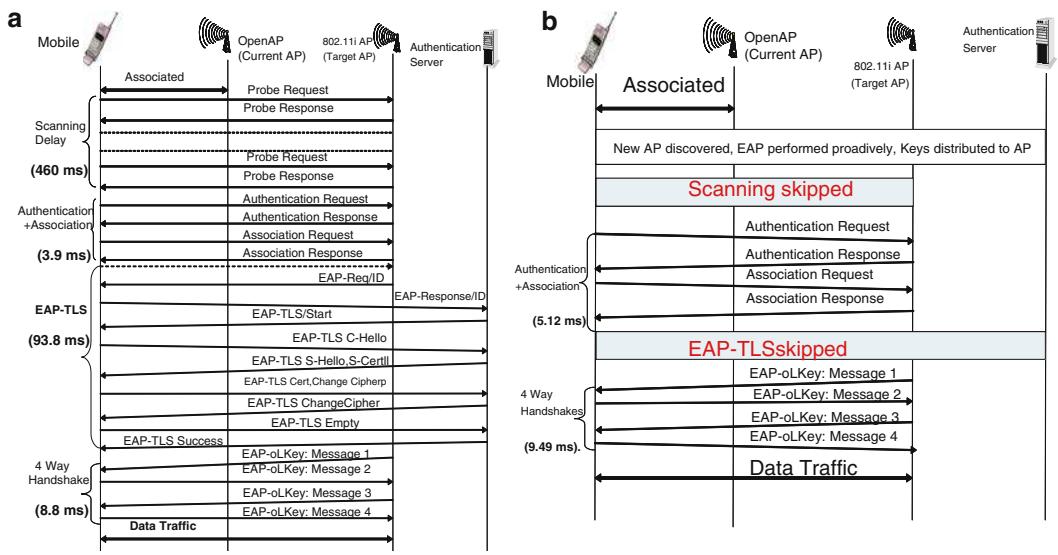

Fig. 7 (**a**) Non-optimized L2 handoff delay. (**b**) MPA-assisted optimized L2 handoff

2 delays of roughly 14.7 ms compared to ~600 ms in the non-MPA case. The results shown in Fig. 7b show the effectiveness of MPA in reducing the layer 2 related configuration during handoff. The reduction of configuration time due to layer 2 pre-authentication is comparable with IEEE 802.11i-based pre-authetication. The MPA scheme looks more attractive for inter-domain movement, since 802.11i-based pre-authentication scheme cannot be applied to situations where the neighboring APs belong to two different domains. Authors have provided a complete analysis of MPA-assisted layer 2 optimization involving inter-domain handover in [19].

A careful breakdown of the handoff timing shows that layer 2 association, authentication and 802.11i 4-way handshake take more or less an equal amount of time in both the cases, but the non-optimized case (Fig. 7a) contributes to more delay because of the additional delay introduced due to layer 2 scanning and EAP-TLS procedure. We also observed that overall layer 2 scanning time is dependent upon MaxChannelTime and MinChannelTime parameters. In our specific experiment, we set the variables "ss_mindwell" and "ss_maxdwell" of MADWIFI driver to 10 ms and 50 ms, respectively and obtained a layer 2 scanning time of 460 ms. These variables correlate with MinChannelTime and MaxChannelTime defined in the 802.11 standard. *Probe-Wait latency* (amount of time a station waits on a particular channel after sending a probe request) depends on these settings. For example, when we changed these values to 20 ms and 200 ms, respectively, total layer 2 scanning time increased to 930 ms. Velayos and Karlsson [35] describe the factors that affect the scanning time and ways of optimizing the scanning time.

We have used "madwifi-ng" drivers with Netgear wireless cards in both the MN and the APs. Hostapd and wpa_supplicant were used in the APs and MN respectively to deploy IEEE 802.11i. Net-snmp was used because it implements SNMPv3 and its security extensions, and finally we have used OpenDiameter to deploy the AAA server functionality that works as a backend server for the PANA Authentication Agent.

The set of three experimental results described in Sects. 5.1, 5.2 and 5.3 highlight the effectiveness of MPA and 802.21 for heterogeneous handover. These results also validate that both MPA and 802.21 can help optimize the handover delay at all layers by optimizing different handover operations such as discovery, network detection, configuration, authentication and binding update.

6 Performance comparison of MPA

In this section we highlight certain added features of MPA that are different than the existing make-before-break techniques. In particular, we compare MPA with FMIPv6 and highlight the functional differences. MPA provides a make-before-break mechanism and takes care of many upper-layer handover related functions leaving only layer 2 handover operation to execute during the move. There are several other proactive schemes, such as MITH [13], FMIPv6 [17] that utilize make-before-break techniques and provide comparable performance.

The distinct features of MPA relative to other related make-before-break schemes are as follows: (1) MPA can work over multiple types of mobility protocols; (2) MPA provides pre-authentication support for both layer 3 and layer 2 thereby reducing the delay due to authentication; (3) MPA provides flexible ways of performing pre-configuration operation such as stateless auto-configuration and stateful pre-configuration using DHCP relay agent; (4) When assisted by IEEE 802.21 information discovery scheme, MPA can optimize the layer 2 handoff by avoiding scanning and IEEE 802.11i authentication; (5) MPA framework can be applied to different types of handover such as inter-domain, intra-domain, inter-technology and intra-technology; (6) MPA provides a flexible buffering mechanism at different parts of the network that can reduce the packet loss during the handover.

Now, we briefly compare MPA with FMIPv6. The IETF has defined two fast-handover protocols for MIPv6, such as hierarchical MIPv6 [34] and Fast MIPv6 [17]. Both of these protocols try to reduce the packet loss and handover delay experienced by the base version of MIPv6. There is a very fundamental difference between MPA and FMIPv6. While FMIPv6 is limited to the use of MIPv6 as a binding protocol for fast-handover, MPA defines a

mobility framework that can work independent of the mobility protocol, and can work with a number of protocols including MIPv4 [27], MIPv6 [16], and SIP-based mobility [31]. However in the context of MIPv6, we provide a brief functional comparison between FMIPv6 and MPA over IPv6.

FMIPv6 provides two ways of providing fast-handoff: predictive mode and reactive mode. The FMIPv6 predictive mode and MPA-based optimization over MIPv6 exhibit some similarities for certain operations such as pre-configuration and proactive binding update. Authors provide a complete overview of MPA operation and the implementation results in the IETF MPA drafts [8] and [23] respectively. Reference [5] provides some experimental results of FMIPv6 that show that delay due to proactive FMIPv6 is bounded by non-optimized layer 2 delay. Similarly MPA over IPv6 is also bounded by non-optimized layer 2 delay in the absence of any assistance from IEEE 802.21's information discovery scheme. According to [5], handover latency for proactive FMIPv6 is equal to layer 2 IEEE 802.11 handover latency and is computed to be 320 ms. On the other hand, MPA assisted by IEEE 802.21 information discovery limits the layer-2 delay to 4 ms by avoiding scanning. FMIPv6 when assisted by IEEE 802.21 information discovery can also help to reduce the layer 2 delay to a comparable value as obtained in the case of MPA.

However there are a few functional differences between MPA over IPv6 and predictive mode of FMIPv6. Below, we list certain functional differences between MPA over IPv6 and FMIPv6.

6.1 Pre-authentication

A key component of MPA over IPv6 is its pre-authentication mechanism. Pre-authentication is a process of authenticating a mobile with the target network from the currently connected network before the mobile moves to the new network [25]. This pre-authentication can take place both in layer 2 and layer 3. Studies [12] show that it takes up to 5 s to complete layer-3 based EAP-AAA authentication. Similarly layer 2 authentication takes up to 600 ms [30] to support IEEE 802.11i in a roaming environment. Although IEEE 802.11i's pre-authentication mechanism can be used to optimize layer 2 pre-authentication it is limited to use within one DS (Distribution System) only. On the other hand, MPA assisted handoff can bootstrap both layer 3 and layer 2 authentication while the mobile is still in the previous network thus optimizing the time taken due to these operations during the handover. This pre-authentication mechanism with the assistance from IEEE 802.21's Information Service helps to bootstrap layer 2 security such as 802.11i and thus optimize the layer 2 delay also. Although FMIPv6 does provide proactive configuration and binding update, FMIPv6 itself does not have any specific pre-authentication mechanism defined as part of RFC 4068. However, recently there has been efforts to add pre-authentication support to FMIPv6 [25], but this support has been removed from the next revised version of the draft. Thus, FMIPv6 when assisted by 802.21 information discovery mechanism can help reduce the handover delay to layer 2 delay but without any security optimization.

6.2 Pre-configuration and binding update

The process of pre-configuration and binding update are also different between MPA over IPv6 and FMIPv6. In the case of FMIPv6, the router of the previous access network and the router of the next access network exchange information to facilitate pre-configuration and fast binding updates before the handover. In MPA,the protocol exchange takes place between the mobile node and the authentication agent, access router (AR) and configuration agent (CA) of the target network. The FMIPv6 protocol exchange between the routers will require some administrative agreement between the neighboring domains and thus FMIPv6 may be more suited for intra-domain case where the routers belong to the same administrative domain. Whereas MPA over IPv6 can work for both intra-domain and inter-domain since the pre-authentication mechanism helps to complete the required pre-configuration and proactive binding updates without any need to have specific protocol exchange between the previous access router (PAR) and next access router (NAR). This alleviates the dependence on the access routers and inter-

communication between the access routers during the handover.

RFC 4068 [17] discusses the mobile's pre-configuration operation. Through RtSolPr and PrRtAdv messages the mobile can formulate a perspective new CoA (nCoA) when it is still in the previous access network. It does not however discuss the use of DHCPv6 to help the configuration process. Whereas MPA over IPv6 does support both modes of pre-configuration, such as stateful configuration using DHCP relay agent and stateless auto-configuration where it can pass the router's prefix over the transient tunnel between the NAR and PAR.

6.3 Auxiliary handoff operations

Additionally, many of the auxiliary handoff operations such as buffering and tunneling are tightly coupled with FMIPv6 signaling, whereas these operations in MPA are not tightly coupled with the signaling of specific mobility protocols such as MIPV6. MPA can make use of binding update mechanisms that come with MIPv6 or any other mobility protocol, whereas pre-authentication, pre-configuration, tunneling and buffering functionalities could be dealt with by separate protocols of choice. For example, in our implementation we have used PANA for pre-authentication and tunnel management and used a newly designed dynamic buffering protocol [9] for buffering packets and reducing the packet loss during handover.

6.4 Support for heterogeneous access handover

Unlike MPA, FMIPv6 in its current form does not provide seamless handover support between heterogeneous access technologies such as CDMA and 802.11. However there is a recent draft [28] that describes the support for handover with heterogeneous access technologies by adding bi-casting with buffering and selective packet delivery technique. MPA does enhance the support for heterogeneous handover by providing a dynamic buffering mechanism and copy and forwarding technique. Details of these techniques are described in [9]. While newly added support for bi-casting and buffering techniques for FMIPv6 are limited to access routers, MPA's buffering mechanism that supports heterogeneous handover is quite flexible as it can be both *time-limited* and *explicit buffering* and its placement is not limited to access router only. The newly designed buffering protocol can be used independent of the mobility protocol used. Additionally, MPA can also be used for situations where the mobile does not need to execute any mobility protocol to support network controlled localized handover [28]. In this situation MPA allows the mobile to use tunnel management protocol to communicate with Next Access Router and provide seamless handoff support between 802.11 and CDMA networks.

Deployment considerations

Besides the operational differences with FMIPv6 for fast-handover, MPA also takes into consideration several deployment scenarios such as failed switch over, ping-pong effect and QOS reservation in the target network during a mobile's movement. More details of MPA can be found in Ref. [8].

Despite certain functional differences between MPA and FMIPv6, MPA's pre-authentication mechanism and stateful pre-configuration mechanism can be used to augment FMIPv6's functionality and further optimize the handover performance.

7 Conclusions

In this paper we have presented a mobility optimization framework that takes advantage of IEEE 802.21 as well as a media independent pre-authentication (MPA) framework to provide secured and seamless convergence and support heterogeneous handover. We have discussed several functional components of the IEEE 802.21 framework and their respective roles in providing the optimization. We explain a laboratory experimental setup where we have implemented several functional components of 802.21 such as the Event Service and Information Service functions, and the MPA technique. The implementation demonstrates network discovery, network selection, pre-configuration, pre-authentication, and proactive handover operations that are part of a mobility

event. We presented the results of two types of heterogeneous handover scenarios: intra-technology, inter-domain; and inter-technology, inter-domain and also demonstrated the effectiveness of MPA-assisted layer 2 pre-authentication. Results obtained from these experiments validate how an MPA assisted IEEE 802.21 framework can provide secured seamless convergence and support different types of heterogeneous handover scenarios by reducing handover delays and packet losses to a level that is acceptable for interactive VoIP and streaming traffic. We also highlight additional features that IEEE 802.21 assisted MPA framework provides compared to other make-before-break techniques including FMIPv6.

References

1. Aboba, B., & Simon, D. (October 1999). PPP EAP TLS authentication protocol. IETF RFC 2716.
2. ANSI/IEEE Std. 802.11 1999 Edition, Wireless LAN medium access control (MAC) and physical layer (PHY) specifications.
3. Bargh, M. S., Hulsebosch, R. J., Eertink, E. H., Prasad, A., Wang, H. et al. Fast authentication methods for handovers between IEEE 802.11 wireless LANs. In: *Proceedings of ACM WMASH 2004*. Philadelphia.
4. Buddhikot, M. M., Chandranmenon, G., Seungjae, H., Lee, Y.-W., & Miller, S. et al . (November 2003). Design and implementation of WLAN/CDMA2000 interworking architecture. *IEEE Wireless Communication* November 2003.
5. Cabellos-Apaicio, A., Nunez-Martinez, J., Julian-Bertomeu, H., Jakab L., & Serral-Gracia, R. et al. (2005). Evaluation of fast handover implementation for mobile IPv6 in a real testbed. IPOM 2005 LNCS 3751.
6. Dutta, A., Madhani, S., Chen, W., Altinas, O., & Schulzrinne, H. (2004). Fast handover schemes for application layer mobility management. In: *Proceedings of IEEE PIMRC*. September 2004, Barcelona, Spain.
7. Dutta, A., Zhang, T., Taniuchi, K., Katsube, Y., Schulzrinne, H. et al. (July 2005). Secured universal mobility for wireless internet, *ACM MC2R*, 9(3), 45–57
8. Dutta, A., (Ed.), Yohba, Y., Fajardo, V., Taniuchi, K., & Schulzrinneh, H. (February 2007). A framework of media-independent pre-authentication. Draft-ohba-mobopts-mpa-framework-04, IRTF MOBOPTS WG, Work in progress.
9. Dutta, A., Famolari, D., Fajardo, V., Ohba, Y., Schulzrinne, H. et al. (2006). Dynamic buffer control mechanism for mobile handoff. IEEE PIMRC September 2006, Helsinki, Finland.
10. Dutta, A., Zhang, T., Ohba, Y., Taniuchi, K., & Schulzrinne, H. (2006). Network discovery mechanisms for fast-handoff. *IEEE Broadnets 2006*, San Jose, CA.
11. Fogelstroem, E., Jonsson, A., & Perkins, C. (October 2006). Mobile Ipv4 regional registration. Draft-ietf-mip4-reg-tunnel-04, IETF work in progress.
12. Georgiades, M. (2004). Context transfer support for IP-based mobility management. CCSR Awards for Research Excellence 2004.
13. Gwon, Y., Fu, G., & Jain, R. (2003). Fast handoffs in wireless LAN networks using mobile initiated tunneling handoff protocol for IPv4 (MITHv4). *IEEE Wireless Communications and Networking* 2003, New Orleans, Louisiana.
14. IEEE P802.21/D04.00. (February 2007). Draft IEEE standard for LAN/MAN: Media independent handover services.
15. Jena Semantic Web Framework, jena.sourceforge.net
16. Johnson, D., Perkins, C., & Arkko, J. (June 2004). Mobility support for IPv6. RFC 3775.
17. Koodli, R. (Ed.) (July 2005). Fast handovers for mobile IPv6. IETF RFC 4068.
18. Levkowetz, H. (Ed.) (October 2006). NETLM protocol, draft-giaretta-netlmm-dt-protocol-02.txt, IETF work in progress.
19. Lopez, R., Dutta, A., & Ohba, Y. Network-layer assisted optimization for secure fast-handoff in 802.11 networks. Submitted to *IEEE Communication Magazine*, Special Issue on Internet Series.
20. Malki, K. (Ed.) (October 2005). Low latency handovers in mobile IPv4. draft-ietf-mobileip-lowlatency-handovers-v4-11 IETF Work in progress.
21. Mishra, A., Shin, M., & Arbaugh, W. (2003). An empirical analysis of the IEEE 802.11 MAC layer handoff process. In: *ACM SIGCOMM Computer Communications Review (ACM CCR)*. (Vol. 33, Issue 2).
22. MADWIFI Driver http://sourceforge.net/projects/madwifi/
23. Narayan, V., Venkitaraman, N., Tschofenig, H., Giaretta, G., & Bournelle, J. (April 2006). Handover keys using AAA. Draft-vidya mipshop-handover-keys aaa-02.txt. IETF Work in progress.
24. Ohba, Y. (Ed), (March 2007). Protocol for carrying authentication for network access (PANA). draft-ietf-pana-pana-14, IETF Draft, work in progress.
25. Ohba, Y. (Ed.) (February 2007). EAP pre-authentication problem statement. draft-ohba-preauth-ps-01, IETF work in progress.
26. Park, S., Kim, P., & Volz, B. (March 2005). Rapid commit option for DHCP v4. IETF RFC 4039.
27. Perkins, C. (Ed.), (August 2002). IP Mobility Support for IPv4. RFC 3344.
28. Petander, H. (October 2006). Bicasting with buffering and selective delivery for fast handovers for MIPv6. draft-petander-mipshop-fmipv6-bbsd-00.txt, IETF Work in progress.
29. RDF Primer, http://www.w3.org/TR/rdf-primer
30. Ruckforth, T. (2004). AAA context transfer for fast authenticated inter-domain handover. Technical Report, September 2004.
31. Schulzrinne, H. & Wedlund, E. (July 2000). Application layer mobility using SIP. *ACM MCR2* 4(3), 47–57.
32. Shin, S., Forte, G., Rawat, A.S., & Schulzrinne, H. (2004). Reducing MAC layer handover latency in IEEE

802.11 wireless LANs. Proceedings of ACM 2004 MOBIWAC, September 2004, Philadelphia, USA.
33. Shin, M., Mishra, A., Arbaugh, W. A., et al. (2004). Improving the latency of 802.11 hand-offs using neighbor graphs. ACM/USENIX International Conference on Mobile Systems, Applications and Services (Mobisys), June, 2004, Boston, MA.
34. Soliman, H., Castelluccia, C., el Malki, K., & Bellier, L. (August 2005). Hierarchical mobile IPv6 mobility management. IETF RFC 4140.
35. Velyaos, H., & Karlsson, G. Techniques to reduce the IEEE 802.11b handoff time. KungiTekniska Hogskolen, Stockholm, Sweden, Technical Report TRITA.
36. Yokota, H., Idoue, A., Hasegawa, T., & Kato, T. (2002). Link layer assisted mobile IP fast handover method over wireless LAN network. *Proceedings of ACM Mobicom 2002*, Atlanta.

Ashutosh Dutta (Senior Member of IEEE and ACM) is currently a Senior Scientist in Telcordia Technology's Internet Network Research Laboratory with an emphasis on mobile networking and middleware applications for the wireless Internet. Prior to joining Telcordia Technologies, Ashutosh was the Director of Central Research Facilities in Columbia University, from 1989 to 1997. His research interests include Session control protocols, Streaming multi-media, wireless multicast, and Mobile wireless Internet. Ashutosh has a BS in EE (1985) from India, MS in Computer Science (1989) from NJIT, and Professional Engineering degree in EE from Columbia University. He is also pursuing his part-time Ph.D at Columbia University. Ashutosh is currently serving as the Vice-chair of IEEE Princeton and Central Jersey section.

Dr. Subir Das is a Senior Scientist in Mobile Networking Department, Applied Research, Telcordia Technologies Inc. Prior to joining Telcordia Technologies, Dr. Das was a faculty member in the E & ECE Department, Indian Institute of Technology, Kharagpur, India. Dr. Das has more than forty publications and three US patents to his credit. He is very active in Standards Organizations and a leading contributor to various Standards. Dr. Das is a TPC member and a tutorial speaker in IEEE and ACM sponsored international conferences. His research interests include mobility management, network security, IP Multimedia Sub-Systems, and ad hoc networking. He is a member of IEEE and a reviewer of IEEE and ACM journals and magazines.

David Famolari is a Senior Scientist and Program Manager within the Applied Research department of Telcordia Technologies. David 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 completed Ph.D. coursework at Columbia University.

Yoshihiro Ohba received a B.E., M.E. and Ph.D. degrees on Information and Computer Sciences from Osaka University, Japan, in 1989, 1991 and 1994, respectively. From 1991 to 2000, he worked in Corporate Research and Development Center, Toshiba Corporation, Kawasaki, Japan. Since 2000, he has been working as a Research Director in Toshiba America Research, Inc., New Jersey, U.S.A.

Kenichi Taniuchi (ktaniuchi@tari.toshiba.com) is working as a researcher in Toshiba America Research, Inc, New Jersey, where he is involved in security and mobility area of Internet wireless communication. He has a Master's degree in Information Science from Waseda Univer-

sity, Tokyo, Japan in 2000. His research interest includes location based application service for mobility.

Victor Fajardo is currently a researcher for Toshiba America Research Inc in New Jersey. His main focus of research is mobility and security. He is involved is standardization work particularly IETF. Prior to that he was a senior engineer for Xebeo communications working on protocol development for core networks specifically traffic engineering. He has also worked in startup companies where he developed IP stacks and related protocols. Victor has completed his Masters degree in Computer Engineering at California Polytechnic University, Pomona.

Rafael Marin Lopez received the M. S. degree in Computer Science from University of Murcia, Murcia, Spain in 2000. In the same year he started as research staff in the Department of Information and Communications Engineering of the University of Murcia on a national e-commerce project named PISCIS. In the end of this project, he followed as researcher in European IST Euro6IX project related with IPv6 from 2001 to 2003. During 2004 he has also worked on European FP6 IST Daidalos project based on Mobility and IPv6. During the end of 2004 until now, he is a full time assistant lecturer in Department of Information and Communications Engineering. Additionally he is collaborating actively in IETF above all PANA WG and HOKEY WG. His main research interests include network access authentication and authorization and related technologies besides of mobility.

Toshikazu Kodama received the B.E., M.E. and Dr.E. degrees in electrical engineering from Tokyo Institute of Technology, Tokyo Japan in 1971, 1973 and 1987, respectively. In 1973, he joined Toshiba Corporation, Kawasaki, Japan, where he has been engaged in the research and development of surface acoustic wave devices, ATM switching systems and mobile communication systems. He is currently the president of Toshiba America Research, Inc. He received the Excellent Paper Award of the IEICE, the Achievement Award of the IEICE, Japan Invention Award, Research Achievement Award from Director General of the Science Technology Agency Japan and IEEE Region 1 Award in 1988, 1995, 1996, 1997 and 2005 respectively. Dr. Kodama is a member of the IEICE and IEEE.

Prof. Henning Schulzrinne received his Ph.D. from the University of Massachusetts in Amherst, Massachusetts. He was a member of technical staff at AT&T Bell Laboratories, Murray Hill and an associate department head at GMD-Fokus (Berlin), before joining the Computer Science and Electrical Engineering departments at Columbia University, New York. He is currently chair of the Department of Computer Science. Protocols co-developed by him, such as RTP, RTSP and SIP, are now Internet standards, used by almost all Internet telephony and multimedia applications. His research interests include Internet multimedia systems, ubiquitous computing, mobile systems, quality of service, and performance evaluation. He is a Fellow of the IEEE.