Integration of IEEE 802.21 services and pre-authentication framework

Miriam Tauil*, Ashutosh Dutta,
Yuu-Heng Cheng, Subir Das, Donald Baker,
Maya Yajnik and David Famolari

Telcordia Technologies, Inc.,
One Telcordia Drive, Piscataway,
NJ, 08854-4151, USA
Fax: +1 732 336 7026
E-mail: miriam@research.telcordia.com
E-mail: adutta@research.telcordia.com
E-mail: yhcheng@research.telcordia.com
E-mail: subir@research.telcordia.com
E-mail: dbaker@research.telcordia.com
E-mail: myajnik@research.telcordia.com
E-mail: fam@research.telcordia.com
*Corresponding author

Yoshihiro Ohba and Kenichi Taniuchi

Toshiba Corporate Research & Development Center 1,
Komukai Toshiba-cho, Saiwai-ku, Kawasaki-shi, 212-8582, Japan
E-mail: yoshihiro.ohba@toshiba.co.jp
E-mail: kenichi.taniuchi@toshiba.co.jp

Victor Fajardo

Toshiba America Research, Inc. (TARI),
One Telcordia Drive, Piscataway,
NJ, 08854-4151, USA
E-mail: vfajardo@tari.toshiba.com

Henning Schulzrinne

Columbia University, 450 Computer Science Building
500 West 120th Street, New York, NY 10027-7003, USA
E-mail: hgs@cs.columbia.edu

Abstract: Providing multi-interface device users the ability to roam between different access networks is becoming a key requirement for service providers. The availability of multiple mobile broadband access technologies together with increasing use of real time multimedia applications is creating strong demand for handover solutions that can seamlessly and securely transfer user sessions across different access technologies. In this paper, we discuss how the

Copyright © 2010 Inderscience Enterprises Ltd.

IEEE 802.21 standard and its services address the challenges of seamless mobility for multi-interface devices. We focus on a proof-of-concept implementation that integrates IEEE 802.21 services and a pre-authentication framework, to optimise handover performance in two different scenarios. The first scenario is initiated by the mobile node and the second one is initiated by the network. We present the measurement results for realising these scenarios. Finally, we describe the implementation challenges and lessons learned through this exercise.

Keywords: IEEE 802.21; MIH; MPA; handover; testbed; heterogeneous network.

Reference to this paper should be made as follows: Tauil, M., Dutta, A., Cheng, Y-H., Das, S., Baker, D., Yajnik, M., Famolari, D., Ohba, Y., Taniuchi, K., Fajardo, V. and Schulzrinne, H. (2010) 'Integration of IEEE 802.21 services and pre-authentication framework', *Int. J. Communication Networks and Distributed Systems*, Vol. 5, Nos. 1/2, pp.172–192.

Biographical notes: Miriam Tauil is a Senior Research Scientist in Telcordia Technologies. Her interests and expertise include mobility management on wireless LANs, handover optimisations using IP signalling protocols such as SIP, Mobile IP and 802.21 (MIH). She received her MS in Computer Science from Columbia University in 1998 and BS from Bar Ilan University, Israel in 1991.

Ashutosh Dutta is a Senior Member of IEEE and ACM and currently Senior Scientist in Telcordia Technologies. Prior to Telcordia, he was the Director of Central Research Facilities in Columbia University, and worked as Computer Engineer with TATAs. He has published more than 70 conference, journal papers, book chapters and internet drafts. He has a BS in EE from India, MS in Computer Science from NJIT, M.Phil from Columbia University, and is a part-time PhD student at Columbia University. He is serving as the Chair of IEEE Princeton and Central Jersey section and Industry Relation Chair for IEEE Region 1.

Yuu-Heng Cheng is a Senior Research Scientist in Applied Research at Telcordia Technologies. She is involved in IEEE 802.21 standards activity. She received her MS in Computer Science and Information Engineering from National Chiao-Tung University in 2001. Her primary research area is policy-based network systems for distributed systems. She is a member of IEEE and ACM.

Subir Das is a Senior Scientist in Applied Research, Telcordia Technologies. He received his PhD in Computer Engineering from IIT, Kharagpur, India. Prior to joining Telcordia, he was a faculty member in IIT, Kharagpur. He leads several research programs in applied research and currently serves as the Vice-Chair of IEEE 802.21 Working Group. His research interests include architecture and protocols in wireless IP networks, mobility optimisation, FMC, IMS, and network security. He has published more than 50 papers and has been granted four US patents.

Donald Baker is a Research Scientist in Telcordia Technologies' Austin Research Center. He earned his PhD from Rice University, Houston Texas, in 1997 in the area of computer supported cooperative work. He also has a Master's in Computer Science and a BS in Electrical Engineering from Rice University. At Telcordia Technologies, he is continuing work in the areas of process-oriented systems and information classification. His main areas of expertise are computer supported cooperative work (CSCW), human-computer interaction, and object-oriented software engineering.

Maya Yajnik is a Senior Research Scientist at Telcordia Technologies specialising in network management system design for IP, Ethernet and MPLS technologies since 2000. She worked with business units to design, develop and deploy network management systems, provided consultation to network operators and worked on government projects for prototyping network management systems for wireless ad hoc networks. She received her PhD and MS in Electrical and Computer Engineering from the University of Massachusetts at Amherst and a BTech in Electrical Engineering from Indian Institute of Technology, Mumbai, India.

David Famolari is a Senior Scientist and Program Manager within the Applied Research department of Telcordia Technologies. David manages operations for joint-research collaboration between Telcordia and Toshiba America Research Inc. (TARI) called ITSUMO that is creating next-generation mobile and wireless technologies. He holds BS and MS in Electrical Engineering from Rutgers University and completed PhD coursework at Columbia University. David has authored numerous technical papers and book chapters and has been granted 13 US patents.

Yoshihiro Ohba is a Research Director in Toshiba America Research Inc. He received his BE, ME and PhD in Information and Computer Sciences from Osaka University in 1989, 1991 and 1994, respectively. He is an active member in IEEE 802 and IETF for standardising security and mobility protocols. He is the Chair of IEEE 802.21a Task Group developing a standard for security extensions to the IEEE 802.21 media-independent handover protocol. He received the IEEE Region 1 Technology Innovation Award 2008 for innovative and exemplary contributions to the field of internet mobility and security related research and standards.

Kenichi Taniuchi is a Research Scientist in Communication Platform Laboratory, Toshiba R&D Center, Japan. He received his BS and MS degrees from Waseda University, Tokyo, Japan, in 1998 and 2000, respectively. Since he joined Toshiba in 2000, he worked in the area of ad hoc networks and Bluetooth for three years. From 2003 to 2007, he was with Toshiba America Research Inc. and worked in ITSUMO project in the area of mobility, network security and standardisation of IEEE802.21.

Victor Fajardo is currently a Researcher for Toshiba America Research Inc. (TARI). His main focus of research is mobility and security. He is currently involved in standardisation work particularly in IETF. Prior to joining TARI, he was a Senior Engineer on Protocol Development for Metropolitan Core Networks specifically in Traffic Engineering. He completed his MS in Computer Engineering from California Polytechnic University, Pomona, USA.

Henning Schulzrinne received his PhD 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 the 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.

1 Introduction

The progress of data networks and wireless devices is making mobile web browsing, banking, social networking, and multimedia entertainment a fact of life today. In addition to the proliferation of various WiFi (2009) access technologies in the unlicensed bands, licensed cellular networks are planning evolutionary paths to support high-rate packet data services including the worldwide interoperability for microwave access (WiMAX, 2009), ultra mobile broadband (UMB, 2009), and long term evolution (LTE, 2009). While debate continues regarding the need for these similar mobile broadband technologies, cost factors, backward compatibility issues, and competing business interests make it unlikely that the industry will converge on a single standard. Therefore, the wireless landscape will remain diverse for the near future, making heterogeneity an important factor for providers and device manufacturers to address.

Device manufacturers are integrating more network interfaces into their devices. Many recent cell phone models support both WiFi and third generation (3G) systems. Laptop computers are emerging with WiMAX, 3G and WiFi modems, as are new classes of devices such as notebooks and mobile internet devices (MIDs). As this multi-interface device trend continues, operators with multiple networks will need to facilitate network access across their multiple systems. Operators who have the ability to switch users' sessions from one access technology to another can better manage their networks and accommodate the service requirements of their users. For example, when the quality of an application running on one network is poor, the application can be transferred to another network where there may be less congestion, lower delays, and higher throughput. Operators can also leverage this ability to manage multiple interfaces to balance traffic loads more appropriately across available networks, improving radio frequency usage, system performance and bandwidth capacity. Supporting seamless and inter-technology handover is a key element to help operators manage and to ultimately thrive from heterogeneity.

IEEE 802.21 (2008) defines a media-independent handover (MIH) framework that can significantly improve handover performance between heterogeneous network technologies. The standard defines the building blocks necessary to exchange information, events, and commands to facilitate handover initiation and handover preparation. The MIH framework cannot be a standalone solution for executing handovers, and needs to be used with a higher layer mobility protocol. The MIH framework can be used with any mobility protocol and therefore can be applied to mobility protocols at the IP-layer, such as mobile IP (Perkins, 2002) and mobile IPv6 (Johnson et al., 2004) as well as to mobility protocols at the application layer such as session initiation protocol (SIP)(Rosenberg et al., 2002).

Many enhancements have been suggested to improve handover performance including mobile IPv6 fast handovers (FMIPv6) (Koodli, 2008), hierarchical mobile IPv6 mobility management (HMIPv6) (Soliman et al., 2005), proxy mobile IPv6 (PMIPv6) (Gundavelli et al., 2008), IKEv2 mobility and multihoming protocol (MOBIKE) (Eronen, 2006), candidate access router discovery (CARD) (Liebsch, 2005) and media-independent pre-authentication (MPA) (Dutta et al., 2009). These enhancements offer mechanisms to improve performance within a specific mobility management protocol. In contrast, the IEEE MIH framework aims to provide tools that can be used

with any mobility management protocol by providing valuable information that can enhance handover execution but also, and perhaps more importantly, handover decision making. By providing detailed information about neighbouring networks as well as information related to link-layer events and policy thresholds, the MIH framework significantly improves situational awareness for both mobile devices and network operators. The greater understanding of network conditions, operator policies and handover candidates would lead to better choices of when and where to initiate handovers.

The MIH framework is link-layer agnostic and defines common APIs that can be reused across mobility managers to access key information. An integrated MIH solution can therefore support handovers across any heterogeneous access technology and can be made to interface with any higher-layer mobility management protocol. These additional benefits make MIH an attractive strategy for carriers who wish to have the flexibility to work with different mobility management strategies.

The MIH framework and its applicability have been addressed by other related work. Melia et al. (2006) simulated an IEEE 802.21 client in a heterogeneous environment and analysed the effect of terminal speed on WiFi 3G handovers but does not provide an experimental validation of those results. An early implementation of IEEE 802.21 with limited functionality was discussed in Dutta et al., (2005). Young et al. (2006) analyse MIPv6 handover delay when MIH services are used. Buburuzan et al. (2007) discuss the integration of broadcast technologies with heterogeneous networks using IEEE 802.21 techniques but do not discuss implementation details. Li et al. (2007) discuss simulations of dual-interface MNs using ns-2 that integrates MIPv4 and MIH. However, to the best of our knowledge there is no previous work that describes the implementation and integration details of the MIH function (MIHF) and media independent pre-authentication using an experimental testbed and operational networks. In this paper, we present a heterogeneous handover solution that integrates MIH and MPA by defining an MIH API that realises the MIH service access point (SAP). We also show detailed sequence diagrams illustrating how the MIH protocol and MIH primitives are used by MPA client and server for the two heterogeneous handover scenarios: mobile-initiated handover and network initiated handover between WiFi and cdma2000 evolution-data optimised (EV-DO) (CDMA, 2009) access networks. Finally, we provide performance results to establish the feasibility of the proposed integration.

The rest of the paper is organised as follows. Section 2 gives an overview of MIH and MPA. Section 3 explains our MIH implementation including several APIs developed to interface with higher and lower layers and our MPA implementation. Section 4 describes the MIH and MPA integration in our testbed as well as two heterogeneous handover scenarios realised in the testbed. Section 5 provides experimental results and performance evaluation based on measurement of the handover preparation latency. Section 6 describes challenges that are identified through the experiment. Finally, Section 7 summarises the paper and indicates possible future directions in this research area.

2 Overview of MIH and MPA

2.1 Media independent handover

IEEE 802.21 is a standard that enables the optimisation of handover between heterogeneous IEEE 802 standard-based systems and may facilitate handover between IEEE 802-based systems and cellular systems (IEEE 802.21, 2008). The IEEE 802.21 standard defines a framework consisting of a MIHF, SAPs and MIH users.

An MIHF provides three types of services for MIH Users:

- the media independent event service (MIES) detects changes in link layer properties and reports appropriate events from both local and remote interfaces, to the MIH users subscribed to these events
- the media independent command service (MICS) provides a set of commands for both local and remote MIH users to control link state
- the media independent information service (MIIS) provides information about neighbouring networks including their location, properties and related services.

An MIHF is a logical entity that provides services for the MIH users through a media independent interface and obtains information from the lower layers via media specific interfaces. MIH services may be either local or remote, with local operation occurring within a protocol stack and remote operation occurring between two MIHF entities. For example, remote communication can occur between an MIHF entity in a mobile node (MN) and another MIHF entity located in a network element, such as a mobility agent.

SAPs define both media independent and media specific interfaces to the MIHF. In particular, the following SAPs are included:

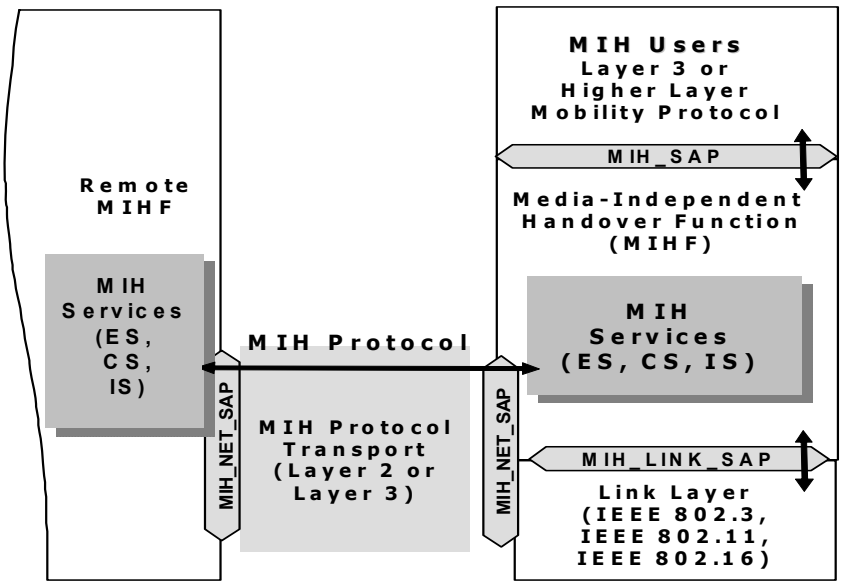
- MIH_SAP: a media independent SAP that provides a uniform interface for higher-layers to control and monitor different links regardless of access technology.
- MIH_LINK_SAP: a media dependent SAP that provides an interface for the MIHF to control and monitor media specific links.
- MIH_NET_SAP: a media dependent SAP that provides transport services over the data plane on the local node, supporting the exchange of MIH information and messages with the remote MIHF.

A set of primitives for these SAPs provide information about their detailed functionality and parameters. Since SAPs and primitives are described in a programming language independent manner, implementations can use any programming language to realise the functionalities provided by the SAPs and primitives.

MIH Users are the functional entities that employ the MIH services to optimise handovers. For example, MIH Users can subscribe to the MIES to be notified when specific events related to handover decision and network selection process occur. Instances of mobility protocols are typical MIH Users.

Figure 1 illustrates the relationship between the MIHF, MIH SAP, MIH link SAP and the MIH user, and the connection between two MIH entities through the MIH net SAP.

Figure 1 MIHF interfaces and communication with a remote MIHF



2.2 Media independent pre-authentication

MPA (Dutta et al., 2009) is a secure handover optimisation framework that allows a MN in the serving network (SN) to securely pre-authenticate and pre-configure itself with a target network (TN) before the handover takes place. With MPA, the MN can establish a Layer 3 connection with the TN before a Layer 2 handover occurs. This process can significantly reduce handover delay and loss by allowing many upper-layer configuration processes to occur before disconnecting with the SN.

MPA provides four basic procedures that are performed by the MN in the SN to help with optimising handover. The first procedure is a pre-authentication in which the MN establishes a security association with the TN to secure subsequent protocol signalling. The second procedure is pre-configuration in which the MN obtains an IP address and other configuration parameters from the TN. The third procedure manage the tunnel and buffer in which the MN establishes a proactive handover tunnel (PHT) with the TN over which IP packets to the TN flow while an access router (AR) in the TN creates a buffer to store in-flight packets. The fourth procedure deletes the PHT when it is no longer needed.

MPA is best suited to support optimisation during handovers where an MN requires a full network access authentication exchange with the home AAA domain of the MN (e.g., a full EAP exchange). Usually this happens either for inter-access network handover or for inter-security domain handover (e.g., between two AAA domains) cases.

MPA defines an authentication agent (AA) and a configuration agent (CA) that resides on the TN to perform the four procedures mentioned above. The authentication agent (AA) is responsible for pre-authentication. An authentication protocol is executed

between the MN and the authentication agent to establish the security association (known as MPA-SA) between the MN and the TN. The authentication protocol derives a key that can be used to mutually authenticate the MN and AA. The CA is responsible for pre-configuration, which involves securely executing a configuration protocol to deliver an IP address and other parameters to the MN. These messages are protected by the key corresponding to the MPA-SA.

In addition, an AR in the TN executes a tunnel management protocol to establish the PHT to the MN and performs buffer management to reduce in-flight packet loss during handover. The signalling messages associated with this tunnel management as well as the IP packets transmitted over the PHT are protected using the key derived from the MPA-SA. A functional implementation of the MPA framework is presented in Dutta et al. (2008) where we used mobility management protocols such as MIPv6 and SIP.

3 Implementation

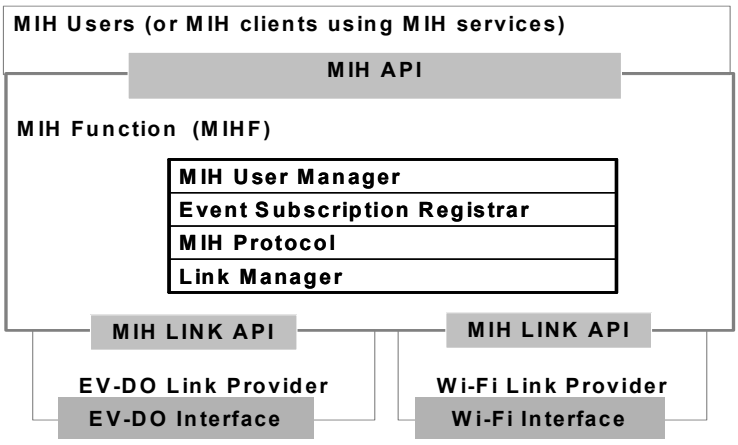
This section describes the software implementations of the MIHF and MPA in our experimental testbed.

3.1 MIH implementation

The MIH software implementation includes the MIHF as well as the MIH IS. The software is implemented in Java 1.6 and is thus portable across different operating systems.

The MIHF software components are shown in Figure 2. The MIH software provides the MIH API for the MIH users. The MIH API embodies the MIH_SAP and supports both local and remote MIH services.

Figure 2 MIHF software components and its interfaces



The physical network interfaces are managed by the link manager via the MIH LINK API.

The MIH LINK API is implemented by the link providers components and embodies the MIH_LINK_SAP. A distinct link provider component is defined for each network

interface type. The link providers are considered as the adapters to the network interfaces and can be implemented either inside or outside of network interface drivers. Our current link providers are implemented outside of the network interface drivers and support MICS and MIES for IEEE 802.11 and cdma2000 EV-DO interfaces in the Linux environment. The link providers are implemented in Java with Java native interface (JNI) to utilise device specific C calls since most device drivers have C APIs rather than Java APIs.

Our link provider implements Link_Parameter_Report event notification, which generates event notifications when the interface crosses configured threshold levels. In order to avoid flooding event notification due to frequently changing signal strength, our link provider implements a function to average the actual signal strength before reporting it to the MIHF. However, this may delay the reaction time on actual threshold crossing.

In the MIHF, the link manager manages the link providers. Communication for remote services is realised by the MIH protocol component. Our current MIH protocol implementation uses UDP as the MIH transport protocol. The Event Subscription Registrar component manages local and remote event subscriptions for the link-layer events monitored by the MIHF. It also aggregates multiple event subscriptions by multiple MIH Users of the same MIHF into a single event subscription and delivers notifications to subscribed MIH Users when event notifications are received.

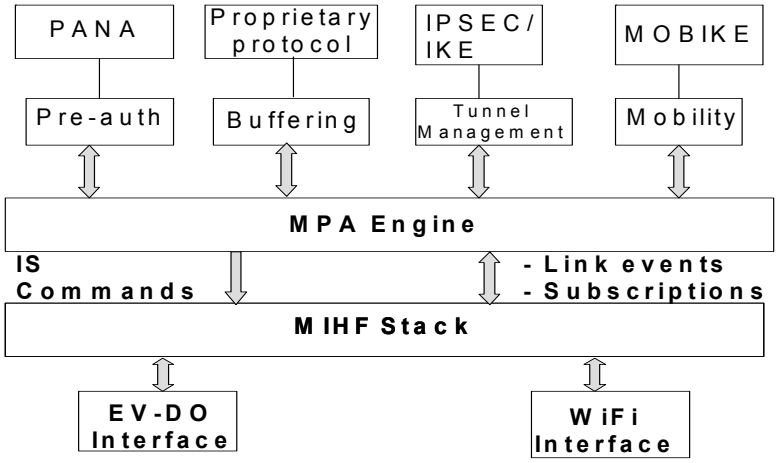
The MIH user manager component is responsible for determining privileges of the MIH users. It enforces coordination between multiple MIH Users such that only one MIH User is allowed to change the state of a specific network interface at a time. This prevents conflicting state changes to be made by different MIH Users that employ different handover policies at the same time. An example could be a network interface that is turned on by one MIH User and then turned off by another MIH User. The IEEE 802.21 information server (IS) is implemented as an 'MIH user' that responds to MIIS queries through interaction with the MIH protocol component. At initialisation, the IS registers with its local MIHF to receive IS queries carried in MIH_Get_Information request messages. After the registration, it is ready to respond to queries sent by other MIH users. Our implementation supports IS queries for resource description framework (RDF) data using SPARQL query language (RDF, 2009). The IS uses an Oracle 11g database to query the RDF data.

3.2 MPA implementation

Figure 3 shows how the MPA engine uses the MIHF and depicts the mapping between MPA functionalities and the protocols of choice in our implementation. Pre-authentication is realised using protocol for carrying authentication for network access (PANA) (Forsberg et al., 2008), a PHT between the MN and the target AR is established using IPSec and IKEv2 (Kaufman, 2005), and buffering is implemented using a UDP-based proprietary protocol. The binding update for the PHT is performed using the MOBIKE protocol since MOBIKE provides an alternate way of providing binding update over a secured tunnel without tearing down the existing security association.

In our MPA framework we use IPsec (Kent and Seo, 2005) IKEv2 and MOBIKE (Eronen, 2006) for managing the PHT mobility.

Figure 3 Interaction between MPA and MIHF



4 Testbed integration and scenario

While the MPA client facilitates the inter-technology proactive handover, the MIH services can provide valuable information to assist in handover preparation and initiation. This section provides detailed information regarding the integration of the MIH and MPA implementation and describes actual handover scenarios from WiFi to EV-DO network using MPA and MOBIKE as the mobility protocol. We describe both mobile initiated and network initiated handovers.

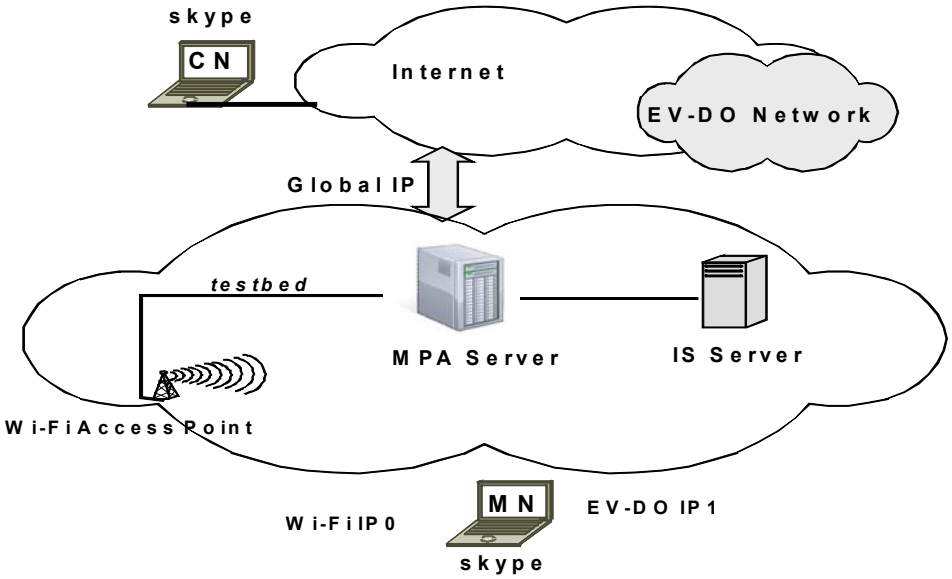
4.1 Testbed setup

Figure 4 depicts the integrated testbed setup. The experimental testbed includes EV-DO and WiFi access networks linked by the internet. The EV-DO service is provided by Verizon Wireless and WiFi networks belong to our enterprise.

The complete testbed consists of the following entities:

- A multi-interface MN. The MN is equipped with WiFi and EV-DO interfaces. The WiFi and EV-DO interfaces have the IP address IP0 and IP1, respectively. The MN runs a MPA client supporting IPsec, IKE, MOBIKE and MIH services. The MPA client uses the MIHF implementation described in Section 3.
- A MPA server is equipped with several modules including an authentication agent (AA), tunnelling agent, CA, and buffering module. It is connected to the internet and the testbed WiFi access point. The AA pre-authenticates the MN. The tunnelling agent handles an IPsec tunnel from the MN as the PHT and performs Layer 3 handover using MOBIKE. Our testbed diverges slightly from the MPA framework (Dutta et al., 2009) in that the tunnelling agent is implemented on a node outside of the TN (i.e., the EV-DO network) not on the AR in the TN because we do not have control of the equipment of the operator's network. As a result, the MPA server acts as a proxy AR to the EV-DO network.

Figure 4 Testbed network layout (see online version for colours)



- An MIH IS contains the testbed network information regarding WiFi access points and cellular network elements. It can be located in any network. For convenience, we have placed it in the testbed network.

- A correspondent node (CN) is connected to the internet and communicates with the MN via the Skype (Skype, 2009) voice over IP session.

In our mobility scenario, the MN engages in a VoIP session with the CN over the WiFi network (path A) and then performs a handover to the EV-DO network (path B). While the MN is still connected to the WiFi network, the MPA engine uses the MIH services to trigger an authentication and configuration process with the EV-DO network in anticipation of the MN's move. The MPA engine learns of the TN by querying the MIH IS for network information. The MPA engine that triggers the authentication can be either on the MN (for mobile initiated) or on the MPA server (for network initiated handover). Although, our demonstration uses signal strength thresholds to trigger the IS query, many other policies may be implemented.

Since the tunnel agent does not reside inside the cellular operator network, all communication to and from the MN needs to go through the MPA server over the PHT, even after L2 handover, as shown in path B.

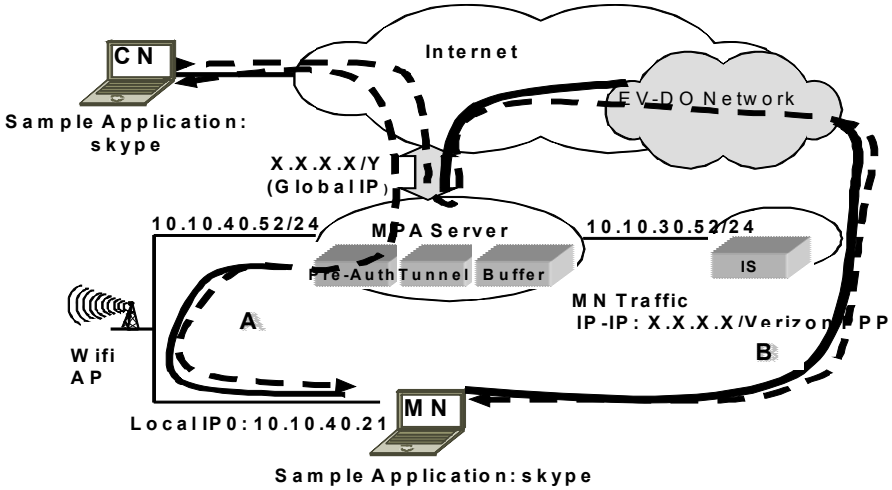
The MPA agents use MIH services for the following purposes:

- Identify when to prepare for handover based on signal thresholds of the active interface. This is done by event subscription to 'parameter reports' when the active interface's signal level in the MN crosses different thresholds.

- Identify candidate networks, and their related parameters, to handover to by querying the information service.

- Using the 'MIH_Link_Actions', power up to connect and configure the EV-DO interface and set up a PHT once pre-authentication procedure is over.
- Using MIH command 'MIH_Link_Actions', power down to turn off the old link once handover is complete.

Figure 5 Data path via WiFi interface (A) and EV-DO interface (B)



4.2 Mobile initiated handover

Figure 6 shows the sequence diagram for a mobile-initiated handover from the WiFi network to the EV-DO network.

The MN is initially connected to the WiFi network. We describe the following steps in sequence.

1 *Subscribe request:* The MPA client first subscribes to the MIH_Link_Parameter_Report event, which provides link parameter reports when the WiFi signal strength crosses certain values.

2 *Configure threshold request*: The MPA client uses a MIH_Link_Configure_Threshold command to establish a set of three WiFi signal strength levels that will trigger notifications. Once a threshold level is crossed, the MIHF will propagate the appropriate notification to the MPA client.

3 *Link parameter report:* When the MPA client receives the first event notification reporting that the WiFi signal strength has crossed below the first threshold, the MPA client prepares for a potential handover, queries the MIH IS (Steps 4 to 5) for available neighbouring networks via the MN's current SN. The IS then sends a response with the information that the cellular network is available (Steps 6 to 7).

8 *Link parameter report:* When the signal strength weakens further and the second threshold is crossed, the MPA client receives an event notification and starts setting up the cellular connection.

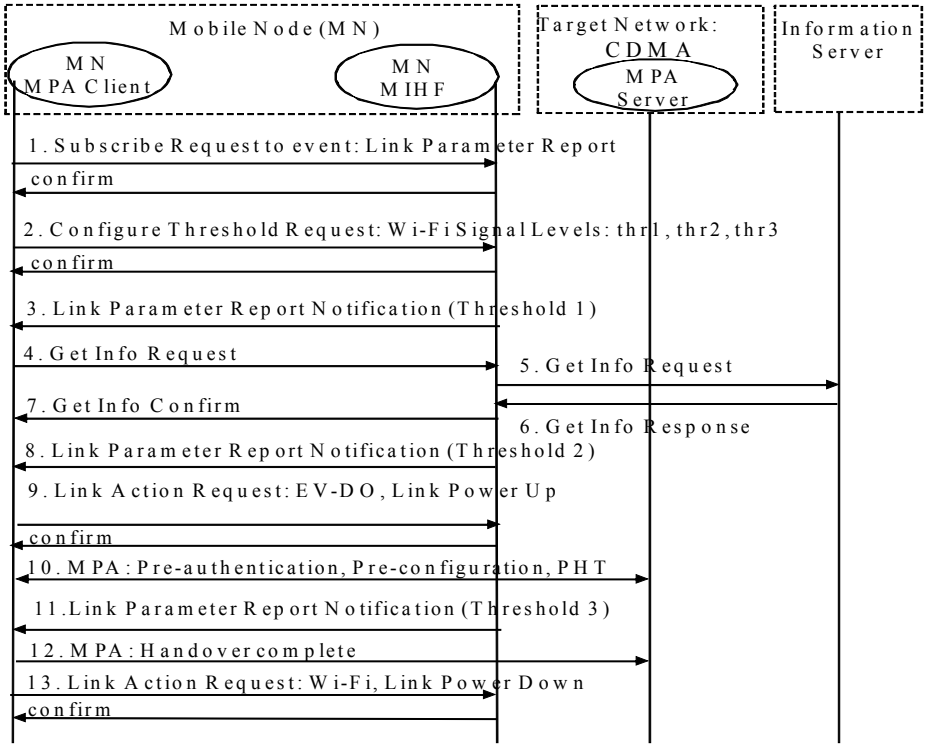
9 *Link up request:* The MPA client brings the EV-DO interface up and establishes an EV-DO connection using a MIH_Link_Actions command. It is important to note that this step can be performed after Step 10 if the IP address to be assigned to the EV-DO interface can be obtained in Step 10, however, this optimisation will require the EV-DO network to support MPA.

10 *MPA proactive handover*: The MPA client starts pre-authentication and pre-configuration through the serving WiFi interface.

11 *Link parameter report*: When the MPA client receives the third link parameter Report event notification, indicating crossing the third lowest threshold value, the MPA client completes the handover operation via MOBIKE address update (12).

13 *Link power down request*: The MPA client then uses a MIH_Link_Actions command to bring down the WiFi interface to conserve the battery power.

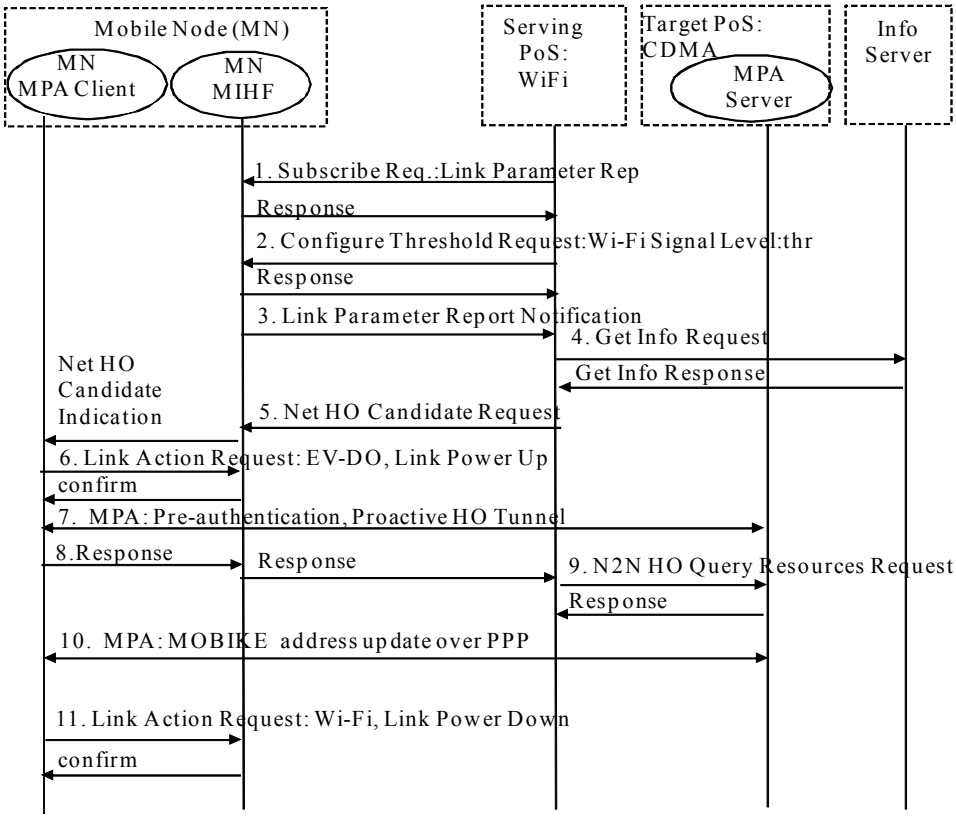
Figure 6 Mobile-initiated handover (WiFi to EV-DO)



4.3 Network initiated handover

Figure 7 shows a sequence diagram for a network-initiated handover from the WiFi network to the EV-DO network. In addition to the entities depicted in Figure 4, a new entity called the serving point of service (PoS) in the WiFi network is used to realise a network-initiated handover.

Figure 7 Network-initiated handover (WiFi to EV-DO)



1 *Subscribe request:* The serving PoS subscribes to the MN to get a MIH_Link_Parameter_Report event notification, which will provide link parameter reports when the WiFi signal strength crosses a given value.

2 *Configure threshold request*: The serving PoS uses a MIH_Link_Configure_Threshold command to configure the WiFi signal strength level that will trigger event notifications. Once a threshold level is crossed, the MIHF in the MN will propagate the appropriate notification to the PoS using the MIH protocol to provide remote event services.

3 *Link parameter report:* When the serving PoS receives the event notification reporting that the WiFi signal strength has crossed the specified threshold, the serving PoS queries the MIH IS as part of Step 4 for available neighbouring networks. The IS then reports that the cellular network is available.

5 *Net HO candidate query request:* The serving PoS sends a MIH_Net_HO_Candidate_Query request message to the mobile indicating the available candidate networks for handover. The candidate networks are selected based on the information obtained from the IS in Step 4.

6 *Link up request:* The MPA client verifies the availability of the cellular network as indicated in the MIH_Net_HO_Candidate_Query request message by bringing the

EV-DO interface up and establishes an EV-DO connection using an MIH_Link_Actions command.

7 *MPA pre-authentication:* Once the target PoS is selected and authentication server is known, the MN contacts the MPA server and starts pre-authentication, and sets up the proactive tunnel through the serving WiFi PoS.

8 *Net HO candidate query response:* Once the EV-DO connection is established, the MPA client responds with an MIH_Net_HO_Candidate_Query response message, indicating the EV-DO network as the candidate network.

9 *N2N HO query resource request/response:* The serving PoS (WiFi) sends the target PoS (CDMA) a network to network (N2N)_HO_Query_Resource request message, to verify that the target PoS has resources before committing the handover. Once the serving PoS get a positive response, it can commit to the handover. While MIH provides a command to indicate handover commitment (i.e., MIH_Net_HO_Commit), we use the MPA proactive handover as the indication of the handover commitment.

10 *MPA proactive handover:* The MPA client completes the handover operation by MOBIKE address update.

11 *Link power down request:* The MPA client then uses a MIH_Link_Actions command to bring down the WiFi interface and conserve the MN battery power.

5 Experimental results

In this section, we explore the MIH signalling flow that trigger the MPA operation in the network initiated handover scenario. We will refer to this MIH signalling flow as *MPA trigger*. We also measure execution time of specific components in the IS and in the MIHF stack in order to understand how the total execution time is distributed among the different operations.

It is important that MIH handover preparation (MPA trigger) and MPA pre-authentication procedures complete before the mobile starts a Layer 2 handover to the TN. The handover preparation time does not directly affect the handover performance and user experience. However, the amount of time the mobile needs to prepare for handover depends upon the speed of the mobile (e.g., pedestrian, vehicular), cell size (e.g., pico cell, macro cell) and type of handover (e.g., single interface, multiple interface). Generally, it is important to reduce the handover preparation time to make the system more resilient to sudden changes in the network characteristics.

This handover preparation time in our experimental scenarios includes the following operational components:

1 propagation of the link events from the link layer to the MIH user (i.e., signal level threshold crossing)

2 querying the IS database

3 MIHF internal operations

4 MPA Layer 3 handover.

The time delays for execution of the operations (2) (3) and (4) were measured, while timing operation (1) will be done in future work.

While we measured delay in the network initiated handover scenario described in Figure 7, some of our measurements apply to other scenarios as well, such as IS transaction processing time and message composition and parsing time.

5.1 Information service transaction delay

We measured different operations in the IS that compose the transaction associated with a request. This sequence starts receiving a *get information request* message containing an IS query and finishes by sending the corresponding response. Table 1 shows five values measured for each operation and their average. The same IS query was used in the samples below.

Table 1 Processing time in the information server (ms)

Measurement #	*1*	*2*	*3*	*4*	*5*	*Average*
Get info request parsing	3	3	4	4	5	3.8
Pass indication from MIHF to MIH user	2	10	2	3	2	3.8
Query processing	5	29	5	25	6	14
Get info response composition	3	2	4	3	2	2.8
Get info response sending	2	1	1	5	2	2.2
Total time processing in the info server						26.6

From the measurements above, we can see that most of the variation in execution time takes place during query processing in the Oracle database. The average IS transaction execution time is 26.6 ms with lower bound of 13 ms and upper bound of 53 ms.

5.2 MIHF implementation performance: MIH message composition and parsing delay

Depending on the MIH message type, the time for message composition and parsing might vary. This depends on the number of TLVs included in each message and the TLV type, which dictates the complexity of its composition and parsing. The average, minimum and maximum of five measurements are presented in Tables 2 and 3, respectively.

Table 2 MIH message composition time

Measurement point	*Message type*	*Execution time**
MN	Link parameter report indication	1.6, 0, 2
Serving PoS	Register response	4.4, 3, 8
Serving PoS	Subscribe request	4.8, 3, 11
Serving PoS	Get info request	6.2, 5, 2
Serving PoS	Net HO candidate request	25.4, 10, 51
Info server	Get info response	2.8, 2, 3

Notes: *Values are in the order of: average, min, max

**Since the resolution of our measurement is 1ms, 0ms means less than 1ms

Table 3 MIH message parsing time (ms)

Measurement point	*Message type*	*Execution time**
MN	NET HO candidate query request	12.6, 6, 19
Serving PoS	Subscribe response	12, 7, 17
Serving PoS	Configure threshold response	40.2, 10, 54
Serving PoS	Link parameter report indication	21.2, 14, 50
Serving PoS	Get info response	11.4, 8, 17
Info server	Get info request	3.8, 3, 5

Note: *Values are in the order of: average, min, max

5.3 MIH performance to trigger MPA procedure in the network initiated handover scenario

We measured the time it took to perform all the MIH operations in our network initiated handover scenario that occurred starting with the initial handover trigger (i.e., crossing signal strength threshold in the MN and creation of the *link parameter report indication*) until triggering the MPA handover operation. Table 4 shows the average execution time of five measurements for each of the specified operations, with the corresponding lower and upper bounds.

Table 4 MIH operation performance before MPA triggering

Measurement point	*Operation description**	*Execution time***
MN	Compose and transmit link parameter report indication (3)	10.4, 10,11
Serving PoS	Receive parse and process link parameter report indication (3)	28.8, 20, 53
Serving PoS	Compose and transmit get info request (4)	14.4, 11, 22
Info Server	Receive parse and process get info request (4)	21.6, 10, 44***
Info Server	Compose and send get info response (4)	5, 3, 9
Serving PoS	Receive parse and process get info response (4)	20, 10, 28
Serving PoS	Compose and send net HO candidate request (5)	31.2, 11, 56
MN	Receive and process net HO candidate request (5)	15.2, 8, 22
	Total	146.6 ms

Notes: *arrow number in Figure 7

**Values are in the order of: average, min, max

***Parse get info request: 3.8ms. Pass get info indication from MIHF to the IS MIH user: 3.8ms. Process IS query in the IS: 14ms

In order to calculate the total MIH MPA triggering operation, we need to add the following network propagation delays:

- MN – serving PoS round trip propagation delay (MN-PoS-RTT).
- Serving PoS – IS round trip propagation delay (PoS-IS-RTT).

In our testbed, we can estimate these delays using round trip ping, which are 1.5 ms for MN-PoS-RTT and 0.3 ms for PoS-IS-RTT, bringing the MIH operation time to trigger MPA to 148.4 ms in the testbed environment.

These round trip propagation delays can be adjusted for a real network environment to estimate a realistic network performance. Since the MN and its serving PoS are relatively close to each other, we estimate their round trip propagation delay, MN-PoS-RTT as 5 ms. We estimate the serving PoS-IS round trip propagation delay, PoS-IS-RTT as 30 ms. In a realistic network the time it would take for MIH to trigger the MPA pre-authentication and handover would be approximately = 146.6 ms + 5 ms (MN-PoS-RTT) + 30 ms (PoS-IS-RRT) = 181.6 ms. This time does not include the propagation of the link event from the link layer to the MIHF, which we have not measured.

5.4 MPA related delays

MPA related delays are attributed to several factors such as delays due to pre-authentication, setting up PHTs and sending the binding update for data redirection. In our testbed, we have measured delays for these components. As shown in Figure 7, pre-authentication and proactive tunnel setup took place before the PPP link was setup. Alternatively, these two operations could take place in parallel with PPP configuration operations that may take up to two to five seconds. Our measurement shows that pre-authentication operation took about 2,175 ms. This time delay consists of several factors, such as four round trip signalling associated with extensible authentication protocol – generalised pre shared key (EAP-GPSK), generation of keys at the authentication server and message processing delays at the end hosts. PHT setup time was measured to be 4,730 ms that includes the time for IKE handshake to set up IPSec tunnel in encapsulating security payload (ESP) (Kent, 2005) mode, and initial MOBIKE exchange. These two operations take place over the WiFi interface in the previous network. Final step in the MPA operation is binding update and it is performed using MOBIKE address update mechanism. It took around 400 ms to complete the round trip MOBIKE signalling over a PPP link.

5.5 Lessons learned from the experiment

An estimation of the MIH handover preparation before triggering MPA in a realistic network is less than 200 ms, which is less than 10% of the time MPA pre-authentication would take. This seems to be a satisfactory time to allow proper triggering time of the MPA operation and handover procedure.

Our measurements of the IS transaction delay and MIHF performance can be used in the future to improve performance of the MIH operations, such as improving query execution time and message parsing time and estimate the MIH signalling execution time for different scenarios.

6 Implementation challenges

A major challenge in trying to reduce the handover preparation time when the TN is the EV-DO network is the lengthy process of setting up a PPP connection that may take

between two to five seconds. Therefore, reducing PPP connection delay is desirable to obtain handover optimisation.

In order to support platform independent porting of the MIHF, we decided to use Java for our implementation. While Java has some advantages for portability, it suffers from performance challenges especially for communication with device drivers. Compiling the Java code into native code may address this issue (Kazi et al., 1999).

The device drivers we investigated do not natively support the link events defined in the IEEE 802.21 specification. The WiFi device driver we used does not expose an interface for triggering MIH link events required by the scenarios. The link provider implementation periodically polls the device status to create the corresponding trigger. For example, the WiFi link provider implementation obtains the signal strength periodically every 100 ms. Then, based on the Link_Configure_Thresholds information, it determines if a Link_Parameter_Report event should be sent to the MIHF. If a short polling period is used, the link provider will consume system resources. On the other hand, if a long polling period is applied, the link provider reaction to triggering a link event will be slow. This issue can be resolved with hardware implementation of the IEEE 802.21 MIH_LINK_SAP.

Similarly, since the EV-DO device driver we used does not have a primitive that supports Link_Parameter_Report event notification, we could not realise the handover scenario that we describe in this paper in the other direction (EVDO to WiFi).As described in Section 4, due to the limitation of not having control of the equipment of the operator's network, the MPA server in our experiment is located outside of the TN acting as a proxy AR. This increases handover latency because one roundtrip exchange is needed between the MN and MPA server after switching to the TN, and there are multiple network layer hops between the two nodes. If the MPA server were implemented on the target AR, this one round trip exchange would have been performed between the MN and target AR that are within the same subnet.

While we populated our MIH IS based on knowledge of the networks in our experiment, the method of gathering the information and populating the database and ability of the MIH entities to securely locate these databases are beyond the scope of the standard. Dutta et al. (2006) explain different ways of populating an IS.

7 Conclusions and future work

In order to make the IEEE 802.21 standard deployable, it is important to gain some insights into how different functional elements can interact with each other in providing seamless communication over a heterogeneous access networks. It is also helpful to learn how choice of different implementation environment such as operating system, programming language and drivers may affect the overall system performance. The implementation of the MIHF and the MIH link SAP for two different link layer technologies as well as the MPA MIH users were instrumental to understand the standard implementation challenges, and identify future research issues to be worked on. Lessons learned from this testbed implementation such as expected handover preparation time can be useful to many of the service providers who plan to integrate IEEE 802.21 technologies with their existing mobility management environment.

The integration of MPA and MIH described in this paper is based on using MPA as an MIH User. A future direction is further integration of MPA and MIH based on moving

some of the functionalities of MPA into the MIHF. Since both MPA and MIH are media-independent, it is a natural step to integrate the two in a single function by extending IEEE 802.21 to support pre-authentication. Not only MOBIKE but also any other mobility protocol can benefit from such an extension to reduce network access authentication latency. IEEE 802.21a, a project under 802.21 working group, is defining extensions to IEEE 802.21 to support pre-authentication and secure the MIH protocol. These extensions will solve the issue with the proxy AR described in Section 6 and protect MIH services from a number of security threats.

Another future direction is for each link-layer technology standard to define link-layer primitives that are mapped to MIH_LINK_SAP primitives so that MIH Users can make use of all MIH_LINK_SAP primitives via MIH_SAP primitives regardless of underlying technologies and hence make MIH a true 'media-independent' layer.

Acknowledgements

The authors would like to acknowledge Dr. Toshikazu Kodama for useful feedback during the course of this work.

References

Buburuzan, T., May, G., Melia, T., Modeker, J. and Wetterwald M. (2007) 'Integration of broadcast technologies with heterogeneous networks – an IEEE 802.21 centric approach', in *Consumer Electronics, ICCE 2007*.

CDMA development Group (2009) '3G – CDMA200 1xEV-DO technologies', online accessed, 11 June, available from World Wide Web, <HYPERLINK'http://www.cdg.org/technology/3g_1xEV-DO.asp'http://www.cdg.org/technology/3g_1xEV-DO.asp>.

Dutta, A. (Ed.), Fajardo, V., Ohba, Y., Taniuchi, K. and Schulzrinne, H. (2009) 'A framework of media-independent pre-authentication (MPA) for inter-domain handover optimization', online accessed, 11 June, available from World Wide Web, <http://tools.ietf.org/html/draft-irtf-mobopts-mpa-framework-05>.

Dutta, A., Das, S., Famolari, D., Ohba, Y., Taniuchi, K., Kodama, T. and Schulzrinne, H. (2005) 'Seamless handoff across heterogeneous networks – an 802.21 centric approach', *IEEE WPMC 2005*.

Dutta, A., Famolari, D., Das, S., Ohba, Y., Fajardo, V., Taniuchi, K., Lopez, R. and Schulzrinne, H. (2008) 'Media independent pre-authentication supporting secure inter-domain handover optimization', *Wireless Communication, IEEE*, April, Vol. 15, No 2, pp55–64.

Dutta, A., Madhani, S., Zhang, T., Ohba, Y., Kenichi, T. and Schulzrinne, H. (2006) 'Network discovery mechanism for fast-handoff', *IEEE Broadnets*, San Jose.

Eronen, P. (Ed.). (2006) *IKEv2 Mobility and Multihoming Protocol (MOBIKE)*, RFC 4555, June.

Forsberg, D., Ohba, Y., (Ed.), Patil, B., Tschofenig, Yegin, A., et al. (2008) *Protocol for Carrying Authentication for Network Access (PANA)*, RFC 5191, May.

Gundavelli, S. (Ed.), Leung, K., Devarapalli, V., Choudhury, K. and Patil, B. (2008) *Proxy Mobile IPv6*, RFC 5213, August.

IEEE 802.21 (2008) 'IEEE P802.21 Std-2008', *IEEE Standard for Local and Metropolitan Area Networks- Part 21: Media Independent Handover Services*.

Kaufman, C. (Ed.), (2005) *Internet Key Exchange (IKEv2) Protocol*, RFC 4306, December.

Kazi, I, Cheng, H., Stanley, B. and Lilja, D. (1999) 'Techniques for obtaining high performance in Java programs', Technical report, University of Minnesota, available at http://www.arctic.umn.edu/papers/java-survey.pdf.

Kent, S. (2005) *IP Encapsulating Security Payload (ESP)*, RFC 4303, December.

Kent, S. and Seo, K. (2005) *Security Architecture for Internet Protocol*, RFC 4301, December.

Koodli, R. (Ed.) (2008) *Mobile IPv6 Fast Handovers*, RFC 5268, June.

Johnson, D. et. al. (2004) *Mobility Support in IPv6*, RFC 3775, June.

Li, M., Sandrasegaran, K. and Tung, T. (2007) 'A multi-interface proposal for IEEE 802.21 media independent handover', *International Conference on the Management of Mobile Business (ICMB 2007)*.

Liebsch, M., Singh, A. (Eds.), Chaskar, H., Funato, D. and Shim, E. (2005) *Candidate Access Router Discovery (CARD)*, RFC 4066, July.

LTE (2009) '3GPP, long term evolution (LTE)', available at http://www.3gpp.org/Highlights/LTE/lte.htm.

Melia, T., de la Oliva, A., Soto, I., Bernardos, C.J. and Vidal, A. (2006) 'Analysis of effect of mobile terminal speed on WLAN/3G vertical handovers', *IEEE Globecom 2006*.

Perkins, C. (Ed.) (2002) *IP Mobility Support for IPv4*, RFC 3220, August.

RDF (2009) 'W3C recommendation, resource description framework (RDF) – concepts and abstract syntax, available at http://www.w3.org/TR/rdf-concepts.

Rosenberg, J. et al. (2002) *SIP: Session Initiation Protocol*, RFC 3261, June.

Skype (2009) available at http://www.skype.com/.

Soliman, H., Castelluccia, C., El Maki, K. and Bellier, L. (2005) *Hierarchical Mobile IPv6 Mobility Management (HMIPv6)*, RFC 4140, August.

UMB (2009) '3GPP2/TSG-C ultra mobile broadband (UMB)', available at http://www.3gpp2.org/Public_html/specs/tsgc.cfm.

WiFi (2009) 'Wi-Fi alliance', available at http://www.wi-fi.org/.

WiMAX (2009) 'WiMAX forum', available at http://www.wimaxforum.org.

Young, Y., Yae, B.H., Lee, K.W., Cho, Y.Z. and Jung, W.Y. (2006) 'Reduction of handover latency using MIH services in MIPv6', *International Conference on Advanced Information Networking and Applications (IANA 2006)*.