Realization of IEEE 802.21 Services and Preauthentication Framework

Miriam Tauil, Ashutosh Dutta,
Yuu-Heng Cheng, Subir Das,
Donald Baker, Maya Yajnik
and David Famolari
Telcordia Technologies Inc.

Yoshihiro Ohba and Victor Fajardo,
Toshiba America Research, Inc.
Kenichi Taniuchi
Toshiba Corporation
Henning Schulzrinne
Columbia University

Abstract — **Providing users of multi-interface devices 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 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, realizing different possible usage scenarios to optimize handover performance. We describe the implementation of two handover scenarios using the 802.21 Services: the first one is initiated by the mobile node and the second one is initiated by the operator network. We compare the two scenarios and discuss their respective benefits. Finally, we describe the implementation challenges and lessons learned through this exercise.**

Keywords-IEEE 802.21; MIH; MPA; handover; testbed; heterogenous network

I. 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 Wi-Fi [1] 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) [2] , Ultra Mobile Broadband (UMB) [3], and Long Term Evolution (LTE) [4]. 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 Wi-Fi and third generation (3G) systems. Laptop computers are emerging with WiMAX, 3G and Wi-Fi modems, as are new classes of devices such as netbooks 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 better 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 [5] 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 higher layer mobility protocols. 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 [6] and Mobile IPv6 [7] as well as to mobility protocols at the application layer such as SIP (Session Initiation Protocol) [8].

Many enhancements have been suggested to improve handover performance including Mobile IPv6 Fast Handovers (FMIPv6) [9], Hierarchical Mobile IPv6 Mobility Management (HMIPv6) [10], Proxy Mobile IPv6 (PMIPv6) [11], IKEv2 Mobility and Multihoming Protocol (MOBIKE) [12], Candidate Access Router Discovery (CARD) [13] and Media-independent Pre-authentication (MPA) [14]. 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 neighboring networks as well as information related to link-layer events and policy thresholds, the MIH framework significantly improves situational awareness for both devices and 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. [15] simulated a IEEE 802.21 client in a heterogeneous environment and analyzed the effect of terminal speed on Wi-Fi/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 [16]. Young An et al. [17] analyze MIPv6 handover delay when MIH services are used. Buburzan et al. [18] discuss the integration of broadcast technologies with heterogeneous networks using 802.21 techniques but do not discuss implementation details. Li et al. [19] discuss simulations of dual-interface mobile nodes 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 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 realizes 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 Wi-Fi and cdma2000 Evolution-Data Optimized (EV-DO) [20] access networks. In the absence of access to any broadband technologies, we used EV-DO. Finally, we provide performance results to establish the feasibility of the proposed integration.

The rest of the paper is organized as follows. Section II gives an overview of MIH and MPA. Section III explains our MIH implementation including several APIs developed to interface with higher and lower layers and our MPA implementation. Section IV describes the MIH and MPA integration in our testbed as well as two heterogeneous handover scenarios realized in the testbed. Section V provides experimental results and performance evaluation based on measurement of the handover preparation latency. Section VI describes challenges that are identified through the experiment. Finally, Section VII summarizes the paper and indicates possible future directions in this research area.

II. Overview of MIH and MPA

A. Media Independent Handover

IEEE 802.21 is a standard that enables the optimization of handover between heterogeneous 802 standard-based systems and may facilitate handover between 802-based systems and cellular systems [5]. The 802.21 standard defines a framework consisting of a MIH Function (MIHF), Service Access Points (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, and
- The Media Independent Information Service (MIIS) provides information about neighboring 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 realize the functionalities provided by the SAPs and primitives.

MIH Users are the functional entities that employ the MIH services to optimize 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.

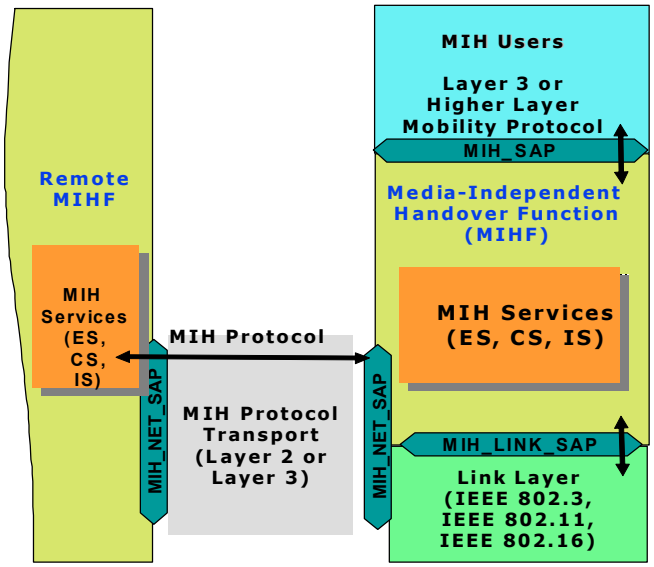

Figure 1. MIHF interfaces and communication with a remote MIHF

B. *Media Independent Pre-Authentication*

Media-independent Pre-Authentication (MPA) [14] is a secure handover optimization framework that allows a mobile node (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 serving network to help with optimizing handover. The first procedure is a pre-authentication in which the MN establishes a security association with the TN to secure subsequent protocol signaling. 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 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 optimization 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 reside on the target network to perform the four procedures mentioned above. The authentication agent (AA) is responsible for pre-authentication. An authentication protocol is executed between the mobile node and the authentication agent to establish the security association (known as MPA-SA) between the mobile node and the target network. 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 mobile node. These messages are protected by the key corresponding to the MPA-SA.

In addition, an access router (AR) in the target network executes a tunnel management protocol to establish the PHT to the mobile node and performs buffer management to reduce in-flight packet loss during handover. The signaling 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 [21] where we used mobility management protocols such as MIPv6 and SIP.

III. IMPLEMENTATION

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

A. *MIH Implementation*

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

1) *MIHF Implementation*

The MIHF software is shown in Fig. 2 and provides the MIH API for the MIH Users. The MIH API embodies the MIH_SAP and supports both local and remote MIH services.

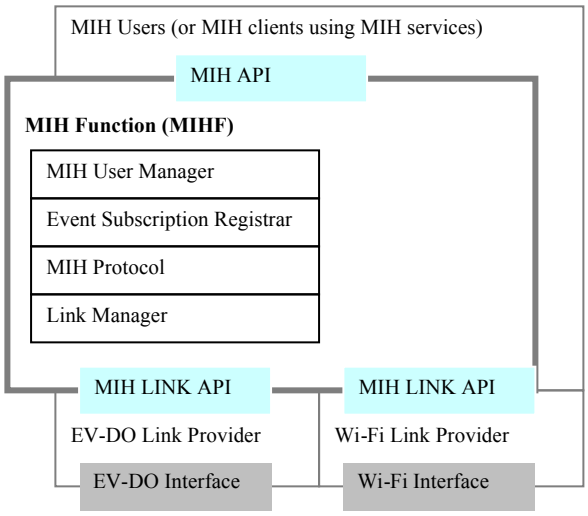

Figure 2. MIHF software components and its interfaces

Communication for remote services are realized by the MIH Protocol component that implements the MIH protocol. Our current MIH protocol implementation uses UDP as the MIH transport protocol.

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.

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 JNI (Java Native Interface) to utilize 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.

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.

2) MIH Information Server (MIIS) Implementation

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 initialization, 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) [22] data using SPARQL query language [23]. The IS uses an Oracle 11g database to query RDF data.

B. 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 realized using PANA (Protocol for carrying Authentication for Network Access) [24], a PHT between the mobile node and the target access router (AR) is established using IPSec and IKEv2 [25], 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 [26], IKEv2 [25] and MOBIKE [12] for managing the PHT mobility.

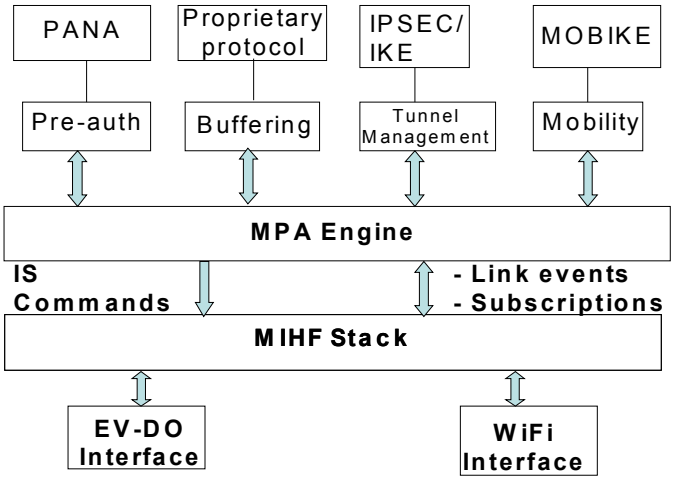

Figure 3: Interaction between MPA and MIHF

IV. 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 Wi-Fi to EV-DO network using MPA and MOBIKE as the mobility protocol. We describe both mobile initiated and network initiated handovers.

A. Testbed Setup

Figure 4 depicts the integrated test-bed setup. The experimental testbed includes EV-DO and Wi-Fi access networks linked by the Internet. The EV-DO service is provided by Verizon.

The complete testbed consists of the following entities:

- A multi-interface mobile node (MN). The MN is equipped with Wi-Fi and EV-DO interfaces. The Wi-Fi 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 III.
- A MPA server is equipped with several modules including an authentication agent (AA), tunneling agent, configuration agent (CA), and buffering module. It is connected to the Internet and the testbed Wi-Fi access point. The AA pre-authenticates the MN. The tunneling 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 [14] in that the tunneling agent is implemented on a node outside of the target network (i.e., the EV-DO network) not on the AR in the target network 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.

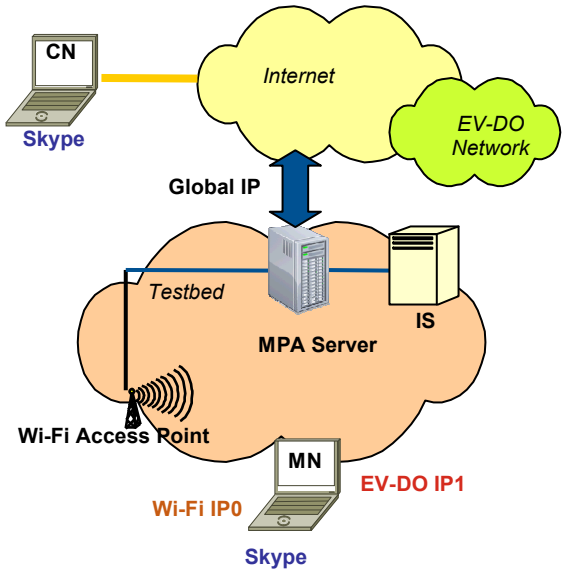

Figure 4. Testbed network layout

- An MIH Information Server (IS) contains the testbed network information regarding Wi-Fi 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 [27] voice over IP session.

In our mobility scenario, the mobile node engages in a VoIP session with the CN over the Wi-Fi network (path A) and then performs a handover to the EV-DO network (path B). While the MN is still connected to the Wi-Fi network, the MPA engine uses the MIH services to trigger an authentication and configuration process with the EV-DO network in anticipation of the mobile node's move. The MPA engine learns of the target network by querying the MIH Information Server 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 MIH command to power up, 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.

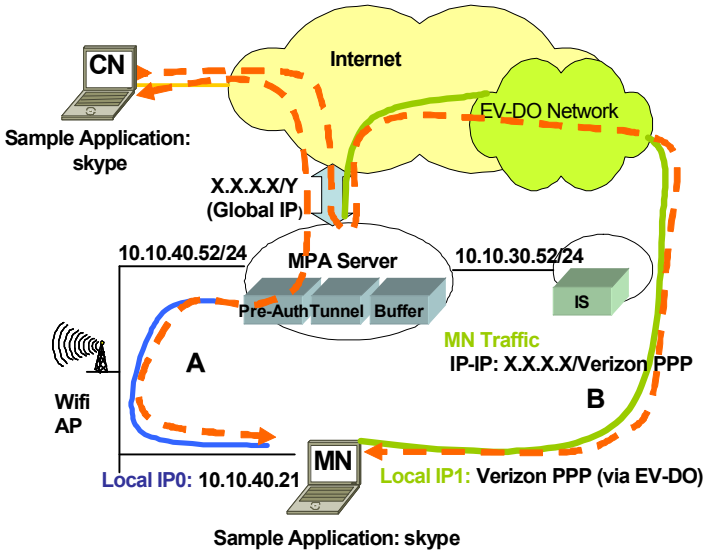

Figure 5. Data path via Wi-Fi interface (A) and EV-DO interface (B)

B. *Mobile Initiated Handover*

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

The MN is initially connected to the Wi-Fi 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 Wi-Fi signal strength crosses certain values.

(2) *Configure Threshold Request*: The MPA client uses an MIH_Link_Configure_Threshold command to establish a set of three Wi-Fi 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 Wi-Fi signal strength has crossed below the first threshold, the MPA client prepares for a potential handover, queries the MIH information server (Steps 4 to 5) for available neighboring networks via the MN's current serving network. The information server 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.

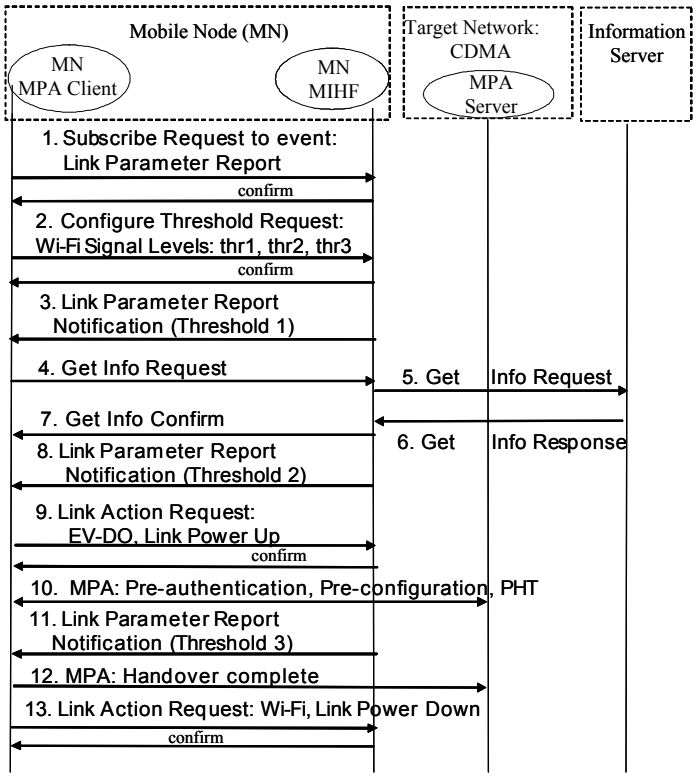

Figure 6. Mobile-initiated handover (Wi-Fi to EV-DO)

(9) *Link Up Request:* The MPA client brings the EV-DO interface up and establishes an EV-DO connection using an 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 optimization 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 Wi-Fi 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 an MIH_Link_Actions command to bring down the Wi-Fi interface to conserve the battery power.

C. Network Initiated Handover

Figure 7 shows a sequence diagram for a network-initiated handover from the Wi-Fi network to the EV-DO network. In addition to the entities depicted in Figure 4, a new entity called the serving PoS (Point of Service) in the Wi-Fi network is used to realize a network-initiated handover.

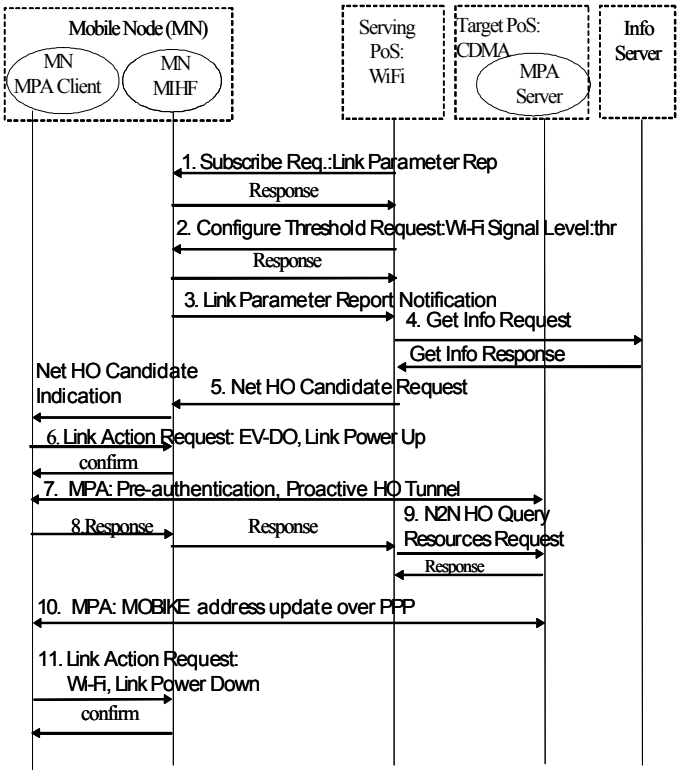

Figure 7. Network-initiated handover (Wi-Fi to EV-DO)

(1) *Subscribe Request:* The serving PoS subscribes to the MN to get an MIH_Link_Parameter_Report event notification, which will provide link parameter reports when the Wi-Fi signal strength crosses a given value.

(2) *Configure Threshold Request*: The serving PoS uses an MIH_Link_Configure_Threshold command to configure the Wi-Fi signal strength level that will trigger event notifications. Once a threshold level is crossed, the MIHF in the mobile node 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 Wi-Fi signal strength has crossed the specified threshold, the serving PoS queries the MIH information server as part of step 4 for available neighboring networks. The information server then reports that the cellular network is available.

(5) *Net HO Candidate Query Request:* The serving PoS sends an MIH_Net_HO_Candidate_Query request message to the mobile indicating the candidate networks available for handover. The candidate networks are selected based on the information obtained from the Information Server 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 mobile node

contacts the MPA server and starts pre-authentication, and sets up the proactive tunnel through the serving Wi-Fi 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 (Wi-Fi) sends the target PoS (CDMA) a N2N(Network to Network)_HO_Query_Resource request message, to verify that the target PoS has resources before committing the handover. Once the serving PoS gets 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 an MIH_Link_Actions command to bring down the Wi-Fi interface and conserve the MN battery power.

D. Analysis and Comparison of the two Handover Scenarios

In this section, we compare and analyze the two handover scenarios.

In the mobile-initiated handover, timing for the initial handover preparation (IS query) is determined by the MN using local MIH services in the MN. This is done by the MPA client in the MN subscribing locally to receive a Parameter Report when the Wi-Fi interface signal level crosses a specified threshold.

In the network-initiated handover, the serving PoS subscribes remotely to receive a Parameter Report when the Wi-Fi interface signal level crosses the specified threshold.

In the mobile-initiated handover scenario, since the MPA client is local to MIHF, it receives notifications of signal level change much faster than the remote serving PoS in the network initiated handover. In the mobile-initiated scenario the handover decision is thus postponed until the active interface signal level crosses a third lower signal level. On the other hand, in the network initiated handover scenario, the first threshold crossing is immediately followed by a signaling sequence to perform the handover. In this case, the additional delays associated with updating the remote PoS make it difficult to respond quickly to deteriorating signals. Therefore, the network-initiated handover process must be more sensitive to deteriorating signal levels than the mobile initiated process.

The serving PoS and target PoS communicate MIH messages (Network to Network Query resource Request/Response) with another to check if the handover can be completed. In our implementation, the target PoS indicates it has the network resources to support the handover.

If the target PoS does not have sufficient resources, the serving PoS would not initiate the MPA handover preparations and the handover would not occur. In the mobile-initiated handover scenario, there is no communication with the target PoS until the MPA proactive handover. The only way to verify that resources in the target PoS are available for the handover is if this check is part of the MPA pre-configuration. In the network-initiated scenario an additional assurance level of the target network availability is provided by the MIH functionality before making the handover decision, which may save time and resources.

The mobile-initiated scenario uses fewer message exchanges than the network-initiated scenario (1 vs. 4). In the mobile-initiated scenario the only message exchange over the network to prepare for the handover is the Get Information request/response, while in the network-initiated scenario the handover preparation includes four message exchanges: Link Parameter Report notification, Get Information request/response, Net HO Candidate Query request/response and N2N HO Candidate Query request/response.

Some network operators may prefer to control the handovers from the network for business and policy reasons. The MIH standards support both implementations and provide operators the flexibility to implement whichever approach best meets their needs.

V. EXPERIMENTAL RESULTS

In this section, we explore the MIH signaling flow that trigger the MPA operation in the network initiated handover scenario. We will refer to this MIH signaling flow as *MPA trigger.*. We also measure execution time of specific components in the Information Server 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 target network. 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:

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

(ii) Querying the IS database
(iii) MIHF internal operations
(iv) MPA layer 3 handover

The time delays for execution of the operations (ii) (iii) and (iv) were measured, while timing operation (i) 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 Information Server transaction processing time and message composition and parsing time.

A. Information Service Transaction Delay

We measured different operations in the Information Server 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 Information Server transaction execution time is 26.6 ms with lower bound of 13 ms and upper bound of 53 ms.

During our measurements, we discovered some anomaly. Thus, we took additional measurement when the information server has been just restarted and connected to the Oracle database. In this case, we discovered that the query processing is much longer, taking an average of 193.2 ms with lower bound of 184 ms and upper bound of 213 ms, considering five measurements. This may be attributed to the fact that it takes time to load the database first time and uses cache next time.

This delay in query processing is dependent on the implementation of the Oracle database and is subject to further study. In this case, query processing time is longer by approximately (193.2-14)=179.8 ms compared to the value in Table 1. Since the MIH Information Server is usually in operation most of the time, this delay rarely occurs and thus not being considered in our analysis.

B. 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 results of five measurements are presented in Tables 2 and 3, respectively.

Table 2: MIH message composing time (ms)

Measurement Point	Message Type	Execution Time (ms) (average, min., max.)
MN	Link Parameter Report Indication	1.6, 0[1], 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

Table 3: MIH message parsing time (ms)

Measurement Point	Message Type	Execution Time (ms) (average, min., max.)
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

C. 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.

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 – Information Server 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 time to trigger MPA to 148.4 ms in the testbed environment.

Table 4: MIH operation performance before MPA triggering

[1] Since the resolution of our measurements is 1 ms, 0 ms means less than 1 ms.

Point of Measurement	Operation Description (arrow number in Figure 7)	Execution time (ms) (average, min., max.)
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) Parse Get Info Request: 3.8 Pass Get Info Indication from MIHF to the IS MIH user: 3.8 Process IS query in the Information Server: 14	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**

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-Information Server 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.

D. MPA Related Delays

MPA related delays are attributed to several factors such as delays due to pre-authentication, setting up proactive handover tunnels 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 2 – 5 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 signaling associated with EAP-GPSK (Extensible Authentication Protocol - Generalized Pre Shared Key), generation of keys at the authentication server and message processing delays at the end hosts. Proactive handover tunnel setup time was measured to be 4,730 ms that includes the time for IKE handshake to set up IPSec tunnel in ESP (Encapsulating Security Payload) [28] mode, and initial MOBIKE exchange. These two operations take place over the Wi-Fi 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 signaling over a PPP link.

E. Lessons 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 timing of the MPA operation and handover procedure.

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

VI. IMPLEMENTATION CHALLENGES

A major challenge in trying to reduce the handover preparation time when the target network is the EV-DO network is the lengthy process of setting up a PPP connection that may take between 2-5 seconds. This challenge is link layer specific and cannot be solved until there is a fundamental change in the link layer technology. In general, reducing PPP connection delay is desirable to obtain further handover optimization.

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 [29].

The device drivers we investigated do not natively support the Link events defined in the IEEE 802.21 specification. The 802.11 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 Wi-Fi 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, the handover scenario that we describe in this paper is not possible to realize in the other direction (EVDO to Wi-Fi).

As described in Section IV, 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 target

network acting as a proxy AR (Access Router). This increases handover latency because one roundtrip exchange is needed between the MN and MPA server after switching to the target network, 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 Information Server 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. [30] explain different ways of populating an information server.

VII. Conclusion 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 MIH Function, 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 learnt 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 environment.

The integration of MPA and MIH described in this paper is based on using MPA as an MIH User. A future direction described below 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. Currently, there is ongoing work in IEEE 802.21 WG to support pre-authentication. This extension will solve the issue with the proxy AR described in Section VI.

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 really "media-independent".

Acknowledgment

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

References

[1] Wi-Fi Alliance, http://www.wi-fi.org/.

[2] WiMAX Forum, http://www.wimaxforum.org.

[3] 3GPP2/TSG-C Ultra Mobile Broadband (UMB), http://www.3gpp2.org/Public_html/specs/tsgc.cfm.

[4] 3GPP, Long Term Evolution (LTE), http://www.3gpp.org/Highlights/LTE/lte.htm.

[5] IEEE P802.21/D14.0, Draft Standard for Local and Metropolitan Area Networks: Media Independent Handover Services, September 2008.

[6] C. Perkins (Ed.), "IP Mobility Support for IPv4", RFC 3220, August 2002

[7] D. Johnson, et. al., "Mobility Support in IPv6", RFC 3775, June 2004.

[8] J. Rosenberg et. al. , "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[9] R. Koodli (Ed.), "Mobile IPv6 Fast Handovers", RFC 5268, June 2008.

[10] H. Soliman, et al.., "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)" RFC 4140, August 2005.

[11] S. Gundavelli (Ed.), "Proxy Mobile IPv6", RFC 5213, August 2008

[12] P. Eronen (Ed.), "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", RFC 4555, June 2006.

[13] M. Liebsch (Ed.), "Candidate Access Router Discovery (CARD)", RFC 4066, July 2005.

[14] A. Dutta (Ed.), "A Framework of Media-Independent Pre-Authentication (MPA) for Inter-domain Handover Optimization," draft-irtf-mobopts-mpa-framework-04, IETF, November 2008, Work in progress.

[15] T. Melia et al., "Analysis of effect of mobile terminal speed on WLAN/3G vertical handovers," IEEE Globecom 2006.

[16] A. Dutta et al. "Seamless Handoff across Heterogeneous Networks – An 802.21 Centric Approach," IEEE WPMC 2005.

[17] Yoon Young An et al., "Reduction of Handover Latency Using MIH Services in MIPv6," Proceedings of the 20th International Conference on Advanced Information Networking and Applications, 2006.

[18] T. Buburuzan, G., May, T. Melia, J. Modeker, M. Wetterwald, " Integration of Broadcast Technologies with Heterogeneous Networks – An IEEE 802.21 Centric Approach", Consumer Electronics, ICCE 2007.

[19] Mo Li, Kumbesan Sandrasegaran, Tracy Tung, "A Multi-Interface Proposal for IEEE 802.21 Media Independent Handover," International Conference on the Management of Mobile Business (ICMB 2007), 2007.

[20] CDMA development Group, "3G – CDMA200 1xEV-DO Technologies", http://www.cdg.org/technology/3g_1xEV-DO.asp

[21] A.Dutta et al., "Media Independent Pre-authentication Supporting Secure Inter-domain Handover Optimization" Wireless Communication, Vol. 15, No 2, pp55 – 64, April 2008.

[22] W3C Recommendation, Resource Description Framework (RDF) – Concepts and Abstract Syntax; http://www.w3.org/TR/rdf-concepts.

[23] W3C Recommendation, SPARQL Query Language for RDF, http://www.w3.org/TR/ rdf-sparql-query/.

[24] D. Forsberg et al., "Protocol for Carrying Authentication for Network Access (PANA)", RFC 5191, May 2008.

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

[26] S. Kent and K. Seo, Security Architecture for Internet Protocol, RFC 4301, December 2005.

[27] Skype, http://www.skype.com/

[28] S. Kent, "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[29] I. H. Kazi et.al., Techniques for obtaining high performance in Java programs," Technical Report, Univesity of Minnesota

[30] A. Dutta et al., "Network discovery mechanism for fast-handoff, IEEE Broadnets, 2006, San Jose.