This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2009 proceedings.

Using the Media Independent Information Service to Support Mobile Authentication in Fast Mobile IPv6

Constantine K. Christakos
Johns Hopkins University
Applied Physics Laboratory
Laurel, MD
dean.christakos@jhuapl.edu

Antonio Izquierdo*, Richard Rouil†, Nada Golmie‡
National Institute of
Standards and Techhnology
Gaithersburg, MD
*aizquier@nist.gov,†richard.rouil@nist.gov,‡nada.golmie@nist.gov

***Abstract*—We explore the use of the Media Independent Information Service (MIIS) in the IEEE 802.21 Media Independent Handover (MIH) framework to improve handover performance for Fast Mobile IPv6 by providing Authentication information. We explore the tradeoffs of Pre-Authentication before joining a new network versus authentication after connecting to a new network during a Fast Mobile IPv6 handover. We discuss our implementations of services available from the MIIS in simulation using the ns-2 simulation system and evaluate their performance.**

I. Introduction

Improving handover performance in mobile networks presents many challenges. Here, we examine methods of improving performance by reducing handover time and consider the role that authentication plays during a handover. The MIH framework[1] was developed in order to facilitate the decision-making capacity of Mobile Nodes (MNs) traveling between PoAs by providing cross-layer information to MNs and Points of Attachment (PoAs). These PoAs may be part of a heterogeneous network, and offer services over WIMAX (IEEE 802.16), WLAN (IEEE 802.11) or UMTS. Frequently we see the MIH used to support signals which indicate a fading or failing link between the MN and PoA[2], indicating to the MN that it needs to seek an alternate PoA in order to maintain its data stream.

The MIIS also serves to facilitate handovers but does so by providing network-wide information to both the MNs and PoAs. For example, the MIIS allows an MN to enter a new network region and receive information about available services and PoA location information, represented as Information Elements (IEs). An MN then has additional information regarding PoA capabilities that fulfills its cost and Quality of Service (QoS) requirements as it moves throughout the network. While there are many pre-existing IEs described in the MIH specification, implementation of the MIH allows for wide latitude, and we present some uses of the MIIS to augment handover decisions. We focus specifically on information that aids the authentication process, providing MNs with authentication information that they would not normally have until they connect to a new PoA.

The rest of this paper is organized as follows: Section 2 provides background on Mobile IPv6 and the MIH and discusses previous work with wireless networks that use the MIH framework, including uses of the MIIS. In Section 3, we discuss the use of the MIIS to augment the authentication process. Section 4 describes the experimental scenarios and results using the MIIS in our implementation. Finally, Section 5 discusses implications of the work and future directions.

II. Background and Previous Work

Fast Mobile IPv6 (FMIPv6)[3] is designed to improve handover performance over Mobile IPv6[4] by assuming that two PoAs during a handover are in close network proximity and allowing them to negotiate a handover and create a network tunnel ahead of time before the MN loses the old connection and makes a new one. The MN starts out connected to a PoA within a subnet managed by an Access Router (AR) (Figure 1a). For our purposes, we regard each PoA as being in a separate subnet and functioning as an AR. With Mobile IPv6, when the MN is away from its "home" network, data addressed to its home destination will be forwarded to the MN by its "Home Agent" (HA), as the MN updates its location with the HA as it moves. FMIPv6 is intended to ensure that the any data interruptions are minimized as the MN travels. A predictive FMIPv6 handover is negotiated by the exchange of messages shown in Figure 2. When the MN discovers the MAC address of a potential new PoA/new AR (NAR), it sends a Proxy Router Solicitation (PrRtSol) to its current PoA/previous AR (PAR) and receives a Proxy Router Advertisement (PrRtAdv) in reply, giving the MN the corresponding IP address of the PoA/AR for the given MAC address that the PAR has stored or otherwise discovers. The MN indicates to the PAR it wishes to begin a handover by sending a Fast Binding Update (FBU) message to the PAR, indicating its planned destination, the NAR, and proposed New Care-of Address (NCoA). The exchange of Handover Initiate (HI) and Handover Acknowledgement (HAck) messages between the PAR and the NAR creates an IP tunnel over which packets for the MN are forwarded to its planned destination (Figure 1b). The

978-1-4244-2948-6/09/$25.00 ©2009 IEEE

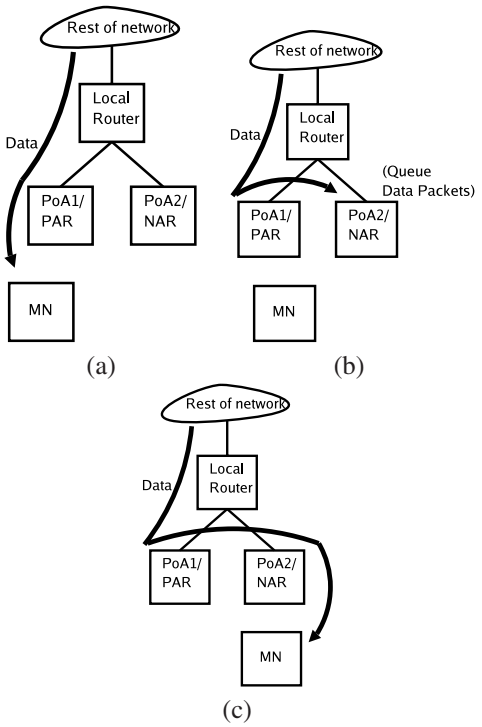

Fig. 1. (a) A mobile node begins at PoA1 and decides to move to PoA2. (b) PoA1 negotiates a handover with PoA2 and begins forwarding its packets to PoA2. (c) When the MN arrives at PoA2, PoA2 releases its buffered packets to the MN.

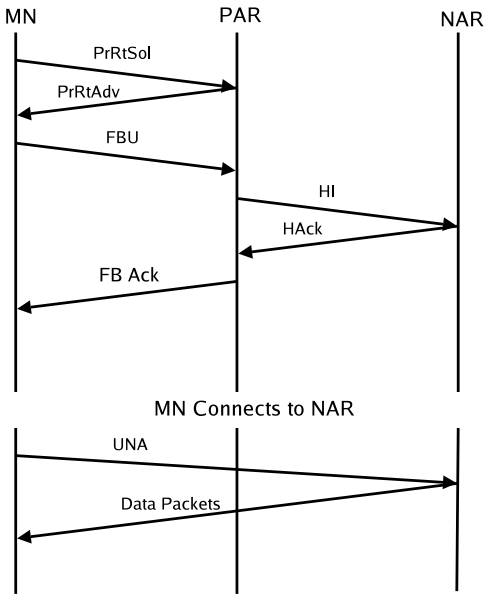

Fig. 2. The exchange of messages in a Fast MobileIPv6 handover

PAR sends a Fast Binding Acknowledgement (FBAck) to the MN, and the MN then connects to the NAR. After connecting, the MN sends an Unsolicited Neighbor Advertisement (UNA) message to the NAR, indicating to the NAR that it can flush its buffer of queued messages and forward future packets on to the MN (Figure 1c). At this point, the MN continues with the normal binding update procedure of Mobile IPv6 in order to redirect packets tunneled by the HA to the PAR to a new IP tunnel between the HA and NAR.

By preemptively forwarding packets to the MN's expected new location, FMIPv6 is designed to prevent packet loss while the MN leaves the PAR and connects to the NAR. The tradeoff is that the MN accepts additional packet delay between receiving the FBAck from the PAR and its sending of the UNA to the NAR. However data loss may occur within this interval if there is a buffer overflow while the NAR was buffering packets tunneled over from the PAR.

The IEEE 802.21 MIH framework is an emerging standard to facilitate seamless handovers between heterogeneous networks. The intent of MIH is to provide link-layer information to the IP-layer in order to faciliate better decision-making when it comes to handovers. In the architecture of the MIH (Figure 3), link-layer information is passed to the MIH Function (MIHF) which passes that information upwards in order to facilitate decision-making. In many instances, these events and decisions are local to the MIH node. For example, a weakening of the connection between an MN and its PoA may generate an MIH "LINK GOING DOWN" event which the MIH User interprets as a signal to scan for another available PoA and connect to it, rather than waiting until the current IP address expires without being renewed by PoA Router Advertisements. In the case of MIPv6, after scanning for an alternative PoA, the MN would attach to the new PoA immediately and send out a BU to its HA, rather than waiting until the connection with its first PoA had timed out before finding a new PoA and re-attaching. MIH also supports remote transmission of messages to other nodes. In the same example as above, the "LINK GOING DOWN" event generated at one node could be transmitted to a remote MIH User at another node, allowing that remote node to make decisions based on the knowledge that the first node is about to leave its network.

Many projects have begun to incorporate the 802.21 MIH as a means of improving handover performance. Mussabbir, et al.[5] incorporate the MIH with FMIPv6 in order to use MIH triggers to provoke predictive FMIPv6 handovers. Their architecture optimizes the FMIPv6 handover process by using the MIIS to provide the MN with mappings of PoA addresses to IP addresses when the MN joins the network, removing the need for the MN to send a Proxy Router Solicitation message as the initial step of the FMIPv6 handover process. Floroiu, et al.[6] discuss the need for a unified MIIS infrastructure that provides information necessary for authorization and QoS information over the network to integrate the MIH into an IP Multimedia Subsystem. Meanwhile, Yoo[7] creates a model based on the assumption that data such as round trip delay between neighbor PoAs is available from the MIIS and can be included in a model of handover time estimation, allowing MNs to make more effective handover decisions based on fine-grain information.

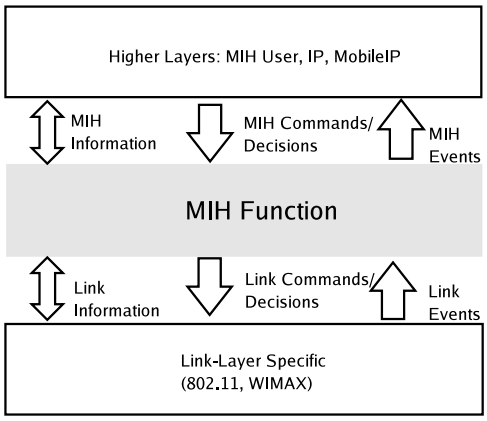

Fig. 3. Basic Architecture of the MIH

III. Using the Media Independent Information Service to Support Authentication

We assume the presence of multiple MIH-capable nodes: the MNs, the Access Routers (ARs), and the Information Server (IS) which contains the MIIS.

We use the Extensible Authentication Protocol (EAP)[8] in conjunction with EAP Pre-Authentication[9] to demonstrate the advantages of using the MIIS. EAP is negotiated as the authentication method for the layer 2 connection between the MN and PoA. Pre-Authentication allows the MN to authenticate with the target while connected elsewhere on the network. EAP Pre-Authentication assumes the MN has knowledge of the new PoA's IP address. With the MIIS, the MN seamlessly and dynamically acquires knowledge of PoA IP addresses, allowing the MN to Pre-Authenticate.

The MIHFs communicate remote events and commands using their unique MIHF IDs. The MIH User and higher layers make the necessary mapping between MIHF ID and network address, and the routing and messaging occurs transparently to the MIHF, which just sends and receives MIH events and commands addressed by ID.

We register the MIHF ID and IP address of the MIIS with each AR in the network. We regard this as a realistic cost of configuration, in the same way that ARs are preconfigured with local DNS, gateway, and DHCP server information. All ARs begin their initialization process by registering with and uploading their network information to the MIIS (Figure 4). The ARs currently register with the MIIS their location, IP address, wireless MAC address, network hop distance to the other ARs, and network hop distance to the network gateway using a proprietary message MIH_Set_Information.request. Users could also pre-populate the AR information in the MIIS.

Each time an MN connects to a PoA and receives a router advertisement indicating it has a new IP address, the MN's MIH makes a capability discovery request to all possible MIHFs available. The AR receives this "Capability Discover Request" and sends back the "Capability Discover Response" indicating that the MN and AR now know each other's capabilities. Finally, the MN registers with the MIHF in the AR. After that process is complete, the MN requests network information data from the MIIS if the capability discover response indicated that this was available.

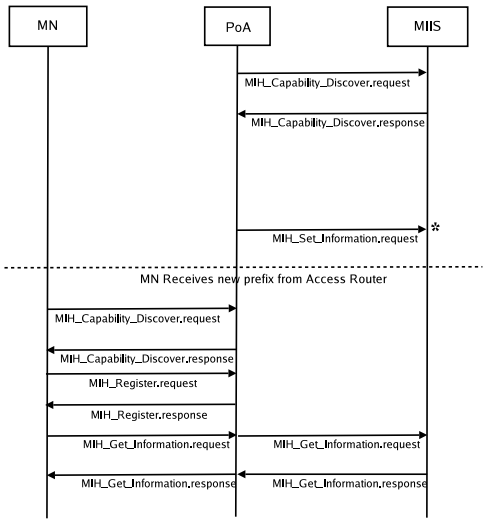

Fig. 4. Message exchange for accessing the Media Independent Information Service. *Note: the MIH_Set_Information.request message is not specified in IEEE 802.21.

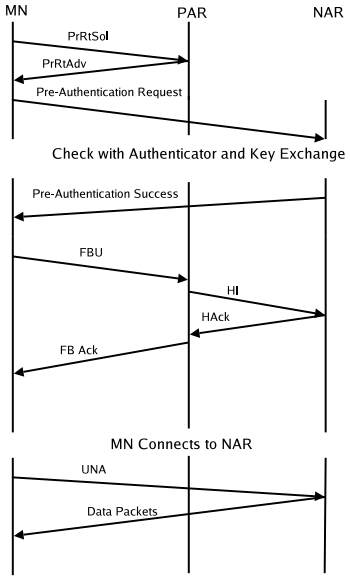

Fig. 5. The exchange of messages when FMIPv6 uses our implementation of Pre-Authentication, without use of the MIIS

Our goal is to see how the MIIS can support improved FMIPv6 performance when combined with security authentication. One can notice parallels between Pre-Authentication and Fast Mobile IPv6: in both cases, the MN is negotiating services with the anticipated PoA ahead of time to ensure that those services will be available when the MN finally connects to the PoA. To integrate EAP Pre-Authentication with FMIPv6, we place the Pre-Authentication process between the reception of the PrRtAdv message and the sending of the FBU. The PrRtAdv message provides the MN with the mapping

between the PoA's MAC and the PoA's IP Address, allowing the MN to send the Pre-Authentication request to the new PoA (Figure 5). Once the MN is notified that Pre-Authentication is successful, it sends the FBU packet to the PAR and connects to the NAR when it receives the FBAck. Because authentication with the destination PoA is already complete, the time it takes to connect to the destination PoA is much shorter, leading to fewer packets queued in the NAR's FBU buffer.

For our analysis, we assume some communication distance between the PoA and the AR. Next, we refer to the previous PoA as the pPoA and the destination PoA as the nPoA. We define the time it takes to send and receive a message "M" to be t_M and the time it takes for a message to travel between node "A" and node "B" to be t_{A-B} (we assume that travel time is equal in both directions). The time to complete a given task "T" is denoted by t_T. Thus, time it takes to begin an FMIPv6 handover (Figure 2) is given by

$$t_{BeginFMIP} = t_{PrRtSol} + t_{PrRtAdv} + t_{FBU} + t_{HI} + t_{HACK} + t_{FBAck}. \quad (1)$$

Expressed in terms of distance between nodes, we have

$$t_{BeginFMIP} = 4t_{MN-pPoA} + 4t_{pPoA-PAR} + 2t_{PAR-NAR} \quad (2)$$

Meanwhile, the time to complete the handover once the FBU tunnel between the PAR and the NAR is established and the FBAck is received is

$$t_{CompleteFMIP} = t_{Connect} + t_{Auth} + t_{UNA} \quad (3)$$

where t_{Auth} is the time it takes the MN to authenticate with the nPoA and $t_{UNA} = t_{MN-nPoA} + t_{nPoA-NAR}$ and $t_{Connect}$ is the time for the MN to complete the other Layer 2 connect operations with the nPoA.

To define t_{Auth}, assume an authentication method requires x initiation and completion messages between the MN and its current PoA and y messages to be exchanged between the PoA and the Authentication Server, which are forwarded between the PoA and the MN. This requires a time of $(x + y)(t_{MN-nPoA} + t_{nPoA-NAR}) + yt_{NAR-AuthServer}$, when MN and nPoA are directly connected, so

$$t_{Auth} = y(t_{MN-nPoA} + t_{nPoA-NAR} + t_{NAR-AuthServer}) + x(t_{MN-nPoA} + t_{nPoA-NAR}). \quad (4)$$

We have implemented a simulated EAP Generalized Pre-Shared Key (EAP-GPSK) authentication method[10] for MN-PoA connections. This requires that the PoA send a request packet to the MN, that a response message from the MN be sent to the Authentication Server via the PoA, and that the Authentication Server and MN exchange four GPSK messages, and completing with a success message sent from the Authentication Server to the MN. Without Pre-Authentication, the factors in Equation 4 give $x = 2$ and $y = 6$, giving

$$t_{GPSKAuth} = 8t_{MN-nPoA} + 6t_{nPoA-AuthServer}. \quad (5)$$

A packet tunneled from the PAR to the NAR takes $t_{PAR-NAR}$ to arrive at the NAR. All data packets that arrive at the PAR after the HAck is received are tunneled to the NAR. Therefore, considering the handover from when the FBAck is sent, if $t_{CompleteFMIP} > t_{PAR-NAR} - t_{MN-pPoA} - t_{pPoA-PAR}$, then the first data packet sent over the FBU Tunnel will remain buffered in the NAR for a duration of up to $t_{CompleteFMIP} - t_{PAR-NAR} + t_{MN-pPoA} + t_{pPoA-PAR}$. Pre-Authentication shortens $t_{CompleteFMIP}$ to $t_{Connect} + t_{MN-nPoA} + t_{nPoA-NAR}$, because the authentication is handled during the beginning of the FMIP process. However, using Pre-Authentication, communication is performed via the PAR, and the total authentication time is $x(t_{MN-pPoA} + t_{pPoA-PAR} + t_{PAR-NAR})$, giving

$$t_{GPSKPreAuth} = 8t_{MN-pPoA} + 8t_{pPoA-PAR} + 2t_{PAR-NAR} + 2(6t_{PAR-NAR}) + 6t_{NAR-AuthServer}. \quad (6)$$

Thus, the additional Pre-Authentication overhead is

$$t_{overhead} = 14t_{PAR-NAR} + 8(t_{MN-pPoA} + t_{pPoA-PAR}) - 8(t_{MN-nPoA} + t_{nPoA-NAR}). \quad (7)$$

IV. Simulation Results

A. Scenario

Using the ns-2 simulator[11], we have developed implementations of the MIH 802.21 and integrated it with our implementation of MIPv6 which supports FMIPv6.

To test the validity of our proposal, we created a simple topology containing an Authentication Server and two PoAs, one supporting IEEE 802.16 (WIMAX) and another supporting 11 Mbit/s 802.11b (WLAN) (Figure 6). The WIMAX model is an ns-2 based model developed at the National Institute of Standards and Technology[12]. The MN here has both 802.11 and 802.16 wireless interfaces. The PoAs and the ARs are combined into the same node, so there is no distinction between the two. For the purpose of calculating predicted handover time, $t_{PoA-AR} = 0$, $pPoA = PAR$, and $nPoA = NAR$.

We examine five scenarios: first, when the MIIS is not used, and there is no Pre-Authentication. Second, when the MIIS is not used, but the MN Pre-Authenticates with the NAR, using the NAR address received in the PrRtAdv. Third, when the MIIS is used to provide IP information about the NAR, bypassing the need for a PrRtSol and PrRtAdv, much like the Optimized FMIPv6 protocol described in [5]. Fourth, when the MIIS is used to bypass the PrRtAdv, as well as using Pre-Authentication before initiating a handover. Fifth and finally, we look at performance when the MN uses the MIIS to Pre-Authenticate itself with *all* of the local PoAs immediately after joining the network and receiving MIIS information. We refer to this as "Universal Pre-Authentication."

When the MN connects to a PoA, it sends an "EAP Start" message to the PoA, which replies with an ID request. Because EAP is a Layer 2 protocol, messaging differs depending on the

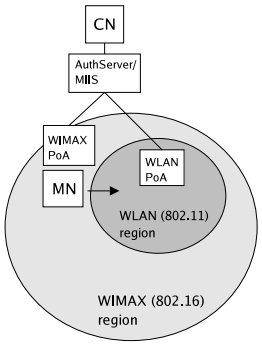

Fig. 6. The topology used for the Pre-Authentication handover experiments.

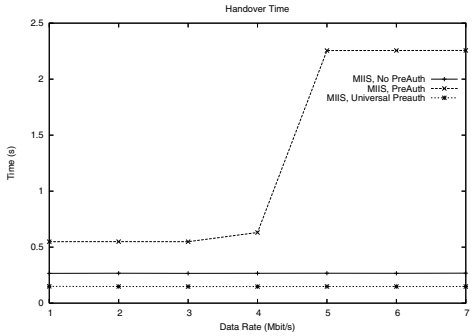

Fig. 7. Handover Time from the MIH LINK DETECTED signal to reception of BAck from the HA

interface. In 802.11, the MN then sends an EAP Association Request to the PoA which begins the authentication process between the server and the MN and completes with a 4-Way Handshake with the PoA. In 802.16, there is no association request, only the authentication process followed by a key download. Once the authentication process is complete, an MIH-enabled MN will raise a "LINK UP" signal. However, the MIH does not have any specific security infrastructure, and during Pre-Authentication, there are no signals that can be raised from the link layer to indicate that the MN's MAC is authenticated with another PoA. The handover module in our MN confirms that Pre-Authentication is complete by periodically polling its MAC.

The two components of the Pre-Authentication overhead in Equation 7 are the communication time between the PAR and the NAR and the difference between the communication time from the MN to the PAR and communication time from the MN to the NAR. Using the topology from Figure 6, assuming 15 ms link delay, communication between the PAR and the NAR during Pre-Authentication will cost an additional 210 ms over conventional EAP Authentication. Assuming that t_{MN-NAR} is negligible, given an uncrowded 802.11 network and that t_{MN-PAR} could be up to 5 ms, the default WIMAX frame duration, this will add an additional 40 ms, giving a total cost of 250 ms. Meanwhile, since $y = 6$, Universal Pre-Authentication should save $6t_{NAR-AuthServer} = 90ms$ compared to standard EAP Authentication. Note that Universal Pre-Authentication is only possible with the MIIS, since the PrRtAdv allows the MN to Pre-Authenticate with the destination PoA/NAR. Since the latency of MN to PoA is low, the gain provided from using the MIIS to bypass the PrRtSol/PrRtAdv is low compared with overall handover time.

Our experiment was designed as follows: the Correspondent Node (CN) sends a Constant Bit Rate (CBR) stream of 188-byte packets to the MN via the WIMAX interface. In this scenario, the MN considers the WLAN interface to be preferable, either because the WLAN provides better bandwidth or the use of a nearby access point is considered preferable, perhaps due to cost. When the MN receives a "LINK DETECTED" signal from the MIH after entering the WLAN region, the MN initiates a fast handover between the WIMAX PoA and the WLAN PoA. We consider the interval between the time at which the MN received a "LINK DETECTED" signal from the MIH when it entered the WLAN coverage area to the time that the MN received a BAck from the Home Agent/WIMAX PoA to be the "total handover time." Within this interval, we examined the number of WIMAX vs. WLAN packets received and the average travel time of those packets between the CN and the MN as throughput increases from 1 Mbit/s to 7 Mbit/s. To confirm that Pre-Authentication is complete, the MN's handover module periodically polls MAC's authentication status with the new PoA/NAR. When the MAC indicates that it is authenticated with the NAR, it sends an FBU message to the PAR (Figure 5). This polling process will time out after 2 s, in which case the MN will continue with the fast handover process and authenticate with the NAR when it connects.

B. Results

The results of our simulations show many of the predicted tradeoffs. Looking at handover times in Figure 7, pre-authenticating with the NAR before connecting takes longer than conventional EAP authentication because of the added communication delay through the PAR. As throughput increases, the data traffic interferes with the Pre-Authentication traffic, and handover time increases to the "time out" threshold of the MN's Pre-Authentication process. For data rates from 1 Mbit/s to 3 Mbit/s, Pre-Authentication results in a handover time of about 548 ms versus a handover time of 265 ms without it. Pre-Authentication adds about 280 ms to the handover time, in line with our expectations. However, by pre-authenticating ahead of time with all PoAs provided by the MIIS, total handover time is reduced considerably, to 150 ms.

This is also borne out with respect to packet queue size during handovers. Without Pre-Authentication, the number of packets queued in the NAR's FBU buffer scales up linearly with bandwidth, as one would expect. While the MN is busy Authenticating with the destination PoA/NAR, packets are buffered at the NAR while awaiting a UNA from the MN after the connection is complete (Figure 8). However, since the connection time is drastically reduced when Pre-Authentication succeeds, no packets need be buffered at the

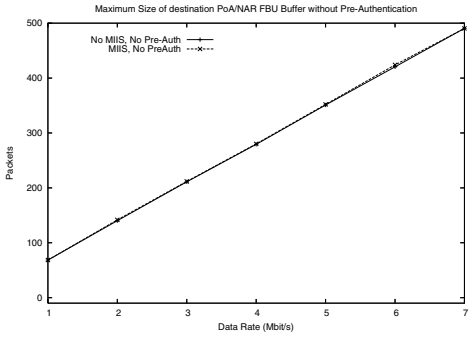

Fig. 8. Maximum Packet Queue Size without Pre-Authentication by increasing bandwidth

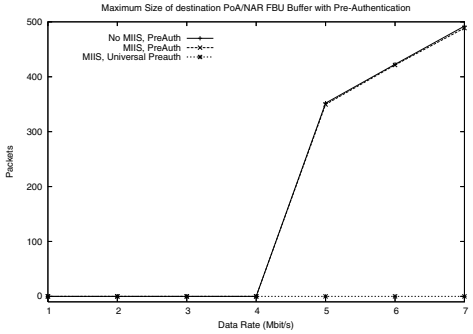

Fig. 9. Maximum Packet Queue Size for using Pre-Authentication by increasing bandwidth

NAR in this case (Figure 9). The flow of packets is seamless with Pre-Authentication, though as bandwidth increases, we see a risk of Pre-Authentication failing to complete due to lost EAP protocol packets between the starting PoA/PAR and the destination PoA/NAR. These losses are typically caused by an overflow of MAC layer queue, with a default maximum value of 50 packets, at the WIMAX base station. Note that the use of the MIIS does not affect the result in the case where the services of the MIIS can be replaced by the PrRtSol/PrRtAdv exchange. Use of the MIIS did reduce overall handover time in WIMAX to WLAN handover, as the PrRtSol/PrRtAdv exchange could add a delay of up to 10 ms.

FBU Tunnel lifetime is reduced with Pre-Authentication because it eliminates the t_{Auth} term, estimated to be 90 ms by Equation 5 in our topology, in Equation 3. Once again, with an increasing data rate, Pre-Authentication cannot complete due to MAC layer queue overflow when the base station attempts to send Pre-Authentication packets to the MN during the fast handover (Figure 10). Reducing FBU Tunnel lifetime ensures that the MN receives data tunneled directly from the HA as soon as possible.

V. Conclusion and Further Work

We have shown some compelling uses of the MIIS to improve Fast Mobile IPv6 performance. Pre-Authentication trades shorter connect time and FBU Tunnel lifetime in exchange for additional overhead in arranging the Fast Handover,

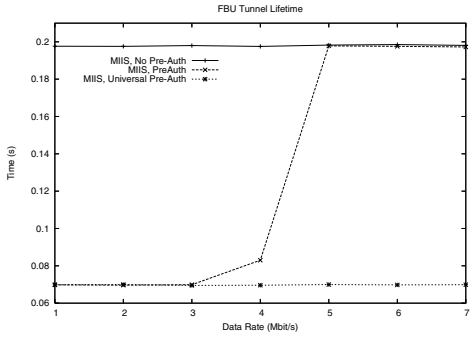

Fig. 10. FBU Tunnel Lifetime with Authentication, Pre-Authentication, and Universal Pre-Authentication

whereas Universal Pre-Authentication using data gathered from the MIIS provides the performance advantages without the increase in Fast Handover time.

Other applications of the MIIS can be used within this framework. MNs could use the MIIS to choose destination PoAs which minimize the number of network hops from their current PoAs, reducing FBU Tunnel lifetime and data packet latency. Another significant open area of interest for continued work is integrating Layer 2 Authentication support for MIH, as opposed to our implementation with a periodic poll of the Layer 2 authentication status to confirm when Pre-Authentication was complete. While other indications about the handover process, such as signal strength, are communicated to the MN in the form of MIH signals, no comparable MIH signals exist for Authentication status. Creating an MIH signal to indicate that an MN has authenticated with a PoA is a natural extension of the work presented here.

References

[1] "IEEE 802.21," http://www.ieee802.org/21.
[2] S. Woon, N. Golmie, and Y.A. Sekercioglu, "Effective Link Triggers to Improve Handover Performance," *Proceedings of the 17th Annual IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2006.
[3] Rajeev Koodli, "Fast Handovers for Mobile IPv6," RFC 4068, IETF, July 2005.
[4] David B. Johnson, Charles Perkins, and Jari Arkko, "Mobility Support in IPv6," RFC 3775, IETF, June 2004.
[5] Q. Mussabbir, W. Yao, Z. Niu, and X. Fu, "Optimized FMIPv6 Using IEEE 802.21 MIH Services in Vehicular Networks," *IEEE Transactions on Vehicular Technology*, pp. 3397–3407, November 2007.
[6] J. Floroiu, M. Corici, Byoung-Joon Lee, S. Lee, S.Arbanowski, and T. Magedanz, "A Vertical Handover Architecture for End-to-End Service Optimization," *16th IST Mobile and Wireless Communications Summit, 2007*, July 2007.
[7] Sang-Jo Yoo, David Cypher, and Nada Golmie, "Timely Effective Handover Mechanism in Heterogeneous Wireless Networks," Tech. Rep., NIST, 2008.
[8] B. Aboba, L. Blink, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)," RFC 3748, IETF, June 2004.
[9] Y. Ohba, "EAP Pre-authentication Problem Statement," Internet-Draft, IETF, June 2008, draft-ietf-hokey-preauth-ps-03.
[10] T. Clancy and H. Tschofenig, "EAP Generalized Pre-Shared Key (EAP-GPSK) Method," Internet-Draft, IETF, July 2008, draft-ietf-emu-eap-gpsk-11.
[11] "Network Simulator – ns-2," http://www.isi.edu/nsnam/ns.
[12] "NIST Project– Seamless and Secure Mobility Tool Suites," May 2007, http://www.antd.nist.gov/seamlessandsecure/doc.html.