Optimizing Authentication in Media Independent Handovers using IEEE 802.21

Antonio Izquierdo, Nada Golmie, Richard Rouil
National Institute of Standards and Technology,
100 Bureau Drive, Stop 8920,
Gaithersburg, MD 20899-8920, USA.
E-mail: aizquier@nist.gov, nada.golmie@nist.gov, richard.rouil@nist.gov

***Abstract*—In this paper we study the performance of the authentication process in media independent handovers and consider the impact of using IEEE 802.21 link triggers to achieve seamless mobility. We describe all interactions between the 802.21 services and the authentication in order to achieve timely and seamless handovers.**

***Index Terms*—IEEE 802.21, Reauthentication, Preauthentication, Media Independent Information Service**

I. Introduction

In today's wireless environment, mobility across different networks is a key characteristic that will become even more relevant as reliable roaming techniques are provided. The main challenge these techniques have to face is the increasing heterogeneity of the wireless technologies, which becomes more important as the user mobility increases. Several mechanisms, tools, and protocols have been devised to minimize the service disruption during the handover process. These tools provide packet buffering at different layers to prevent packet loss, notifications about the optimal timing for starting the handover process, and information about the target network. By using all these enhancements, it is possible to reduce the time required to perform the network selection and parameter negotiation (e.g., the security parameters).

Authentication plays a significant role during handover, as the cryptographic operations involved make this a resource-demanding process that involves a series of message exchanges between the mobile node and an authentication peer (e.g., an authentication server). Additionally, optimizing the authentication is not an easy process, as we have to take care of maintaining the security level of the original protocol and deal with the security principles that drive the security protocols' design. Furthermore, the actual authentication performance is very dependent on the hardware platform, which makes it very hard to predict beforehand the time required to complete the authentication. Given that many proposed mechanisms for providing seamless handovers rely on the knowledge of the required authentication time, as in [16] and [1], authentication introduces an additional problem in the way of seamless handovers.

In this paper we consider two optimizations of the authentication process that are based on the Extensible Authentication Protocol (EAP) framework ([2]), namely reauthentication ([11]) and preauthentication ([14]), and we will analyze their performance in the context of media independent handovers. We also review how the use of the IEEE 802.21 specifications ([6]) can improve the authentication performance by providing information about the current network and potential targets and how this interaction can enable the use of both reauthentication and preauthentication simultaneously. We present simulation results obtained using the NS-2 [13] simulator, with extensions for IEEE 802.16 and IEEE 802.21 [12].

The remainder of this paper is organized as follows. In section II we review the authentication process in wireless networks and the optimizations aforementioned, and in section III we introduce the relevant services and mechanisms of IEEE 802.21. In section IV we describe the simulation environment, scenarios, and parameters used for our study. Section V presents the results obtained in our simulations, while in section VI we present our conclusions.

II. Authentication in wireless networks

In this section we provide a brief overview of the authentication process in heterogeneous networks and the optimizations that are technology dependent. We also review the strengths and issues of each of these optimizations.

In a wireless network the layer 2 authentication of the mobile node (MN) is achieved by using an authentication protocol between the MN and an authentication server. Once the MN is successfully authenticated, both the MN and the Point of Attachment (PoA) derive cryptographic information to protect the subsequent communications. The authentication protocol can be chosen among those defined for each technology, which means that the results of the authentication cannot be shared among PoAs that use different technologies (e.g., IEEE 802.11 and IEEE 802.16), as the cryptographic requirements and operations are different for each of them. This has lead to several technology-specific optimizations of the authentication process as a part of optimized horizontal handovers. The most notable examples are 802.11r ([8]) and 802.16e ([7]).

This technological isolation is partially solved by the use of EAP. EAP provides a framework to perform an authentication exchange that is totally independent of the underlying media. As such, it can be used for layer 2 authentications (as it is in 802.11 and 802.16), layer 3 authentications (e.g., in the Internet Key Exchange (IKEv2) protocol used in IPsec [9]) or user applications. Although the operations performed with the

security information exchanged using EAP may differ between technologies, the information resulting of an EAP authentication is always the same, which makes it possible to design authentication optimizations that are media independent.

The two authentication schemes studied in this paper are the reauthentication proposal based on the Handover Keying IETF Charter (HOKEY) key hierarchy, and the proposal for preauthentication using the existing connection ([14]). The main idea behind the reauthentication is that, by using media independent authentication mechanisms, the resulting information can be shared among different networks (thus, avoiding the need to perform full authentications over and over again). This is achieved by reusing the master key negotiated between the MN and the authentication server and deriving a new key hierarchy that fits the requirements of the new network.

On the other hand, indirect preauthentication is driven by the idea that the MN may know the destination PoA in advance, so it can carry out the authentication (using layer 3 messages if needed) before having to perform the handover to the new network (thus, reducing the handover time). In this case, the MN will perform the authentication exchange with the target PoA before the network entry takes place, thus removing this phase from the actual network entry during the handover.

As we can see, both of these optimizations will provide a significant improvement of the handover performance, as long as the MN can access the required information in time. In the case of the reauthentication, the MN needs to know if the target network will support the reauthentication process and whether the target authentication server will accept to reuse the current cryptographic information.[1] For preauthentication, however, the information required is even more significant, as the MN needs to know the target network, which may use a different technology than the current network. Although some technologies have mechanisms to inform the MN about neighbor networks, they can only provide information about PoAs of the same kind, so an external service is required. This is the point where IEEE 802.21 can provide valuable information.

III. IEEE 802.21 Services

The latest draft of IEEE 802.21 defines a component in the network stack called the Media Independent Handover Function (MIHF) that interacts with the different network layers through the gathering and dissemination of information and commands. This draft provides three different services that help to manage the interfaces and connections during handovers. These services are the Media Independent Command Service (MICS), the Media Independent Event Service (MIES) and the Media Independent Information Service (MIIS). In this paper we focus on the MIES and the MIIS.

The goal of the MIES is to provide information about link related events through the use of link triggers. These triggers notify the node of the loss of connectivity in the current link

[1]This usually means that the target network belongs to the same authentication domain or has an agreement with that of the current network.

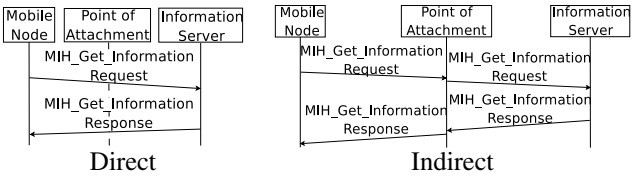

Fig. 1. Message flows for the access to the IS by the MN

(*Link Down (LD)* trigger), the establishment of a connection in a given interface (*Link Up (LU)* trigger), and the progressive loss of the current link (*Link Going Down (LGD)* trigger). This last trigger serves as a notification of the progressive degradation of the link quality, which will likely become a full loss of connectivity.

The MIIS provides information about the networks (current and neighbors) that range from the location of the PoAs to the capabilities in several aspects with security being one of them. In a network environment that uses 802.21 to help handovers, the Information Server (IS) can inform an MN about items like the capabilities of target networks, the domain they belong to and their location, so the MN can take an optimal decision about which target PoA it will attach to when it needs to perform a handover. This information can be static or dynamic: the static information would contain configuration parameters or hardware preconfiguration, while the dynamic information is learned and can be modified as the network conditions change.

This IS can be accessed by an MN in two different ways: directly or indirectly. When contacting the IS directly, the MIHF of the MN sends an '`MIH_Get_Information Request`' message to the IS, which replies with the requested information in an '`MIH_Get_Information Response`' message. Additionally, the MN can request the information to their current PoA instead of querying the IS. If the PoA has this information, it will send the reply to the MN; otherwise, the PoA will query the IS itself, learning the information it receives in the '`MIH_Get_Information Response`' and sending the response to the MN. In this way, the MN has accessed the information in the IS indirectly. The message flows for both types of access are shown in Figure 1. Note that in the indirect access, the request sent by the PoA to the IS is not the same request received from the MN, but the PoA creates a new request based on the message received from the MN and the information it already knows.

The information that is available through the MIIS encompasses network topology (e.g., the networks that surround the current one), administrative organization (for example, roaming partners of the current network provider), technical capabilities (such as the channel used or the authentication methods supported), quality of service parameters, etc. In order to only retrieve the information that is of interest in each moment, the MN may provide filters in the information request, limiting both the specific information the MN is interested in (e.g., the authentication optimizations supported by the networks), and the networks about which the information

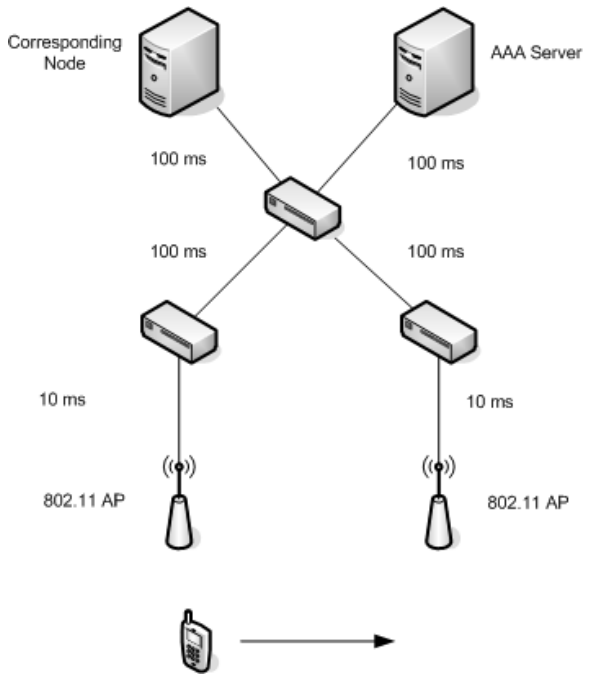

Fig. 2. Network topology

is requested (either by providing a condition such as 'neighbor networks for this PoA', or a list of network IDs). These flexible filtering capabilities make it possible to efficiently manage all the information available through the MIIS.

IV. Simulation Environment

In this section we present the simulation environment used to analyze the performance of the authentication in heterogeneous networks, as well as the metrics used.

Our simulation results were obtained using the NS-2 simulator, with extensions for the IEEE 802.21, the authentication schemes described previously and Fast Mobile IPv6 (FMIPv6, [10]). Fast Mobile IPv6 supports node mobility across networks both in predictive and reactive modes, so it will help to study the effect of predictive optimizations like preauthentication and some link triggers. For this study we will make use of IPv6 ([4]) stateless address autoconfiguration, defined in [15].

Our basic scenario is shown in Figure 2, where we can see two wireless networks using 802.11, and an MN moving from one to the other. The evaluation could use heterogeneous networks (e.g., by including a 802.16 network) and a multihomed mobile node, but in that case we would not be able to appreciate the differences in the disruption time, as in the optimal handover the second interface would connect to the target network before losing the current link, regardless of the authentication method used. We can see in the backbone network the corresponding node that will be sending a constant bit rate (CBR) traffic to the MN, and the Authentication server (AAA server) with which the MN will have to perform the L2 authentication during the handover. In order to better isolate the effect of each authentication optimization in the handover performance, only L2 authentication is considered, i.e., L3 authentication is not required in this scenario. In this scenario both wireless networks belong to the same authentication domain, so it will be possible to use the authentication optimizations previously discussed. Whenever an optimization is not supported, the MN will perform a full authentication to connect to the network. The MN and the AP use 802.1X to transport the authentication messages, which are encapsulated in RADIUS messages between the AP and the AAA server.

TABLE I
Simulation parameters

802.11 coverage area radius	50 m
Key lifetime	More than the simulation time
Size of Diffie-Hellman keys	1024 bits
Size of symmetric keys	128 bits
Size of EAP IDs	64 bytes
Time required to complete DH key generation	2 s
Interval between consecutive Router Advertisement	2 s
Network prefix lifetime	18 s
Application traffic type	Constant Bit Rate
Application traffic rate	10 kB/s
Application traffic bursts	500 B every 50 ms

The authentication methods used in our simulations are the Generalized Pre-Shared Key (EAP-GPSK, [3]), which is a lightweight symmetric key method, and Tunneled TLSv1 with MD5 challenge-response (EAP-TTLSv1-MD5, [5]), a more complex and elaborated authentication method, based on asymmetric cryptography. We have to note that the Diffie-Hellman key generation required for the completion of the TTLSv1 authentication is a very demanding operation, especially for mobile nodes that do not have powerful processors. These methods will provide us with information about the general performance of these two families of authentication mechanisms.

The MN is an IEEE 802.21 compliant entity, which means that it has an MIHF and can make use of the different IEEE 802.21 services and mechanisms. In this study we use the 802.21 link triggers to enable FMIPv6 predictive mode: If the MN makes use of the link triggers, when the MIHF receives the LGD indication, it commands the MN to perform the network discovery, after which the FMIPv6 module starts the handover in predictive mode and the authentication optimizations (if any) are performed. The mechanism used to trigger the LGD indication is the one proposed by Yoo et al in [16]. Furthermore, the MN may use the 802.21 Information Service to gather information about the authentication methods, target networks, etc. In case the MN does not use link triggers, FMIPv6 is used only in reactive mode, and the authentication optimizations (if any) are started based on other information about the target network. How the MN acquires this data is out of the scope of this paper (some possibilities include the data being be preloaded in the MN and the use of other information services).

The specific simulation parameters used to configure the scenario can be seen in Table I.

TABLE II
DISRUPTION TIME(ms)

	Full Auth.	Reauth.	Indirect Preauth
GPSK	19970.3	19970.1	19970.1
TTLSv1-MD5	23511.8	19970.1	19970.1

TABLE III
AUTHENTICATION SIGNALING LATENCY(ms)

	Full Auth.	Reauth.	Indirect Preauth
GPSK	888.23	225.74	3.44
TTLSv1-MD5	3832.37	225.74	3.44

TABLE IV
HANDOVER DELAY (ms)

	Full Auth.	Reauth.	Indirect Preauth
GPSK	2890.13	2889.96	2891.01
TTLSv1-MD5	4910.12	4899.98	4905.25

TABLE V
DISRUPTION TIME WITH LINK TRIGGERS(ms)

	Full Auth.	Reauth.	Indirect Preauth
GPSK	1264.39	610.45	580.49
TTLSv1-MD5	4335.42	610.45	580.49

In order to measure the optimizations in the authentication process, we will focus our analysis on the **service disruption time**. The service disruption time is the time between the reception of the last packet in the old network and the reception of the first packet in the new network. This metric will tell us how the user's applications are affected in the different situations. However, whenever they help us to better understand the results, we will use other metrics: the handover delay and the authentication signaling latency. The handover delay is the time elapsed since the MN decides to switch to a new network until the MN is ready to transmit and receive data packets through the new link. The authentication signaling latency is a measure of the time since the first message of the authentication procedure is sent, until the last message of this authentication process is received.

Additionally, in order to provide the simulator with realistic information about the cryptographic performance, we used as an example a Palm Tungsten C[2] to obtain the time required to compute all the cryptographic operations. Although the performance results of the cryptographic processing are dependent on the choice of platform used, and may therefore vary from system to system, the relative gain or loss in performance between different authentication schemes remains valid for any platform choice.

V. PERFORMANCE RESULTS

In this section we present the results obtained in the simulation of handovers using the described optimization mechanisms. We analyze the performance gain when using the optimized authentication schemes with no other handover optimization mechanism. Next we analyze the performance of handovers that make use of the link triggers defined in 802.21, with and without optimized authentication procedures. Finally, we will study the possibility of using the information services available through the 802.21 Information Service to use all the authentication schemes in the optimal way.

A. Authentication optimizations

Firstly we review the disruption time during a handover when using the different authentication schemes. We can see the simulation results in Table II[3]. We notice that there are no significant differences between the different schemes when using GPSK; only when using TTLSv1 we notice an improvement in the disruption time. Although it seems that the authentication schemes are not actually improving the performance, let us look at the authentication signaling latency, shown in Table III.

Here we can see how both reauthentication and preauthentication are improving significantly the time required to perform the authentication during the handover, but this improvement does not affect the disruption time. If we look at the handover delays (shown in Table IV), we can see that the handover delay is not affected either by the authentication scheme used. However, these handover delays are much lower than the disruption times, which means that most of the disruption time happens while the MN is not aware that it has lost the current connection. Once its network prefix expires, the MN starts the handover process, and after performing the network entry in the new network, it still has to wait for the scheduled Router Advertisement messages. These delays are so long that they make the improvements in the authentication signaling mostly irrelevant.

B. Handovers using 802.21

Our next step in this study is to use of the mechanisms provided in 802.21 in order to optimize the handover process in general and to evaluate the performance of the authentication schemes in this optimized environment. The use of link triggers will allow FMIPv6 to use its predictive mode, and prevent packet loss by instructing the target Access Router to buffer the packets addressed to the MN until the handover process is complete. The disruption time is the time elapsed between the indication to the current Access Router to redirect the traffic to the target Access Router and the request to get all the buffered packets. The values obtained in our simulations can be seen in Table V. As we can see, using the optimized authentication schemes provides a significant improvement, reducing the disruption time of the full authentication to less than half.

[2]This device was used as an example platform, and its use in this research does not constitute an endorsement by National Institute of Standards and Technology

[3]Note that the computation of the Diffie-Hellman agreement in TTLS took 3384 ms on the Tungsten platform chosen

TABLE VI
DISRUPTION TIME WITH LINK TRIGGERS AND MIIS(ms)

	Full Auth.	**Reauth.**	**Indirect Preauth**
GPSK	924.39	270.45	210.49
TTLSv1-MD5	3995.42	270.45	210.49

Furthermore, the use of link triggers and the optimized authentication schemes makes the authentication signaling latency (which is the same as we saw in Table III) reduce its importance. By comparing the values in Table III and Table V we see that the signalling latency in a full authentication represents more than 70 % of the disruption time, while reauthentication only represents 37 % and preauthentication a mere 0.6 %.

We can see how the combined use of optimized mobility protocols, authentication mechanisms and link signaling can improve the overall handover performance more than the improvement that can be provided by any of these proposals on its own. However, this situation is still not optimal, as the MN can make use of the MIIS to gather the information needed before it decides to handover to a new network. By using the MIIS to provide information about the neighbor networks before starting the handover process, the MN can reduce even more the disruption time and eliminate the need for scanning. We can see in Table VI that the gain in our simulations range from the 6 % in the case of full authentication with TTLSv1, to the 60 % reduction in the case of preauthentication. This again shows that the individual improvements of each optimization are boosted when combined with other optimizations.

C. Integrating the authentication schemes through the use of 802.21

Focusing again on the authentication process, the use of the MIIS gives the MN the possibility to learn about the neighbor networks and their capabilities. This is very important not only to know what authentication scheme to use, but also to choose the one that provides optimal results. In the case of the authentication schemes studied in this paper, reauthentication would be optimal when performing handovers in the same authentication domain, as its performance is very similar to that of preauthentication but it reduces the cryptographic operations. Preauthentication, on the other hand, is optimal when entering a new authentication domain, as reauthentication cannot be used in this situation. Furthermore, preauthentication can be used to authenticate with the first network of a domain that an MN detects (or is informed about its existence), so that the MN can use reauthentication whenever it wants to move to that domain.

To illustrate the advantages of combining both methods, we will use a new scenario, shown in Figure 3, where the MN will follow the path illustrated by the arrow while moving across several overlapping networks of different domains. The networks with the same border (solid, dashed or dotted) belong to the same domain, while those in solid color are those to

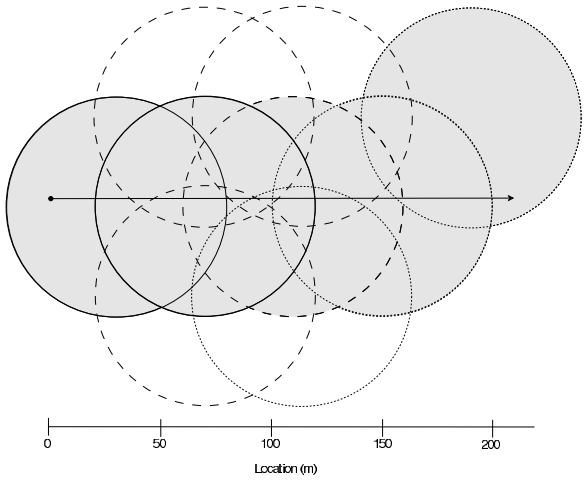

Fig. 3. Network topology for evaluating the optimized authentication scheme

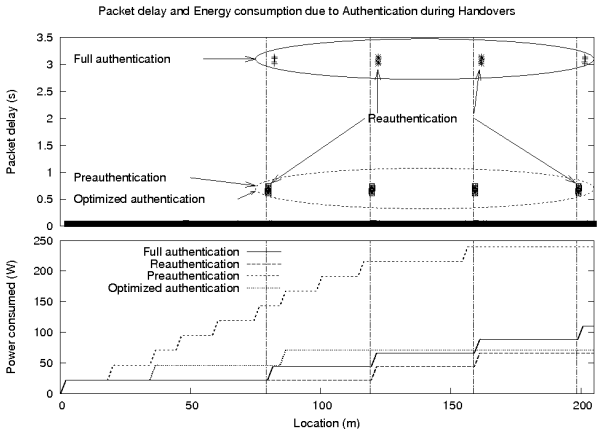

Fig. 4. Packet delay and energy consumed in the authentication

which the MN will actually connect. During the simulation the MN can choose to connect to any network available.

In Figure 4 we can see the comparison of the packet delay and the energy consumed by the different authentication schemes discussed in this paper and the results for the optimized version that combined both optimizations with the 802.21 triggers and the MIIS. We can see how the optimized solution minimizes the delays during handovers (marked by the vertical lines) in every handover, as happens when using only preauthentication. The use of full authentication provides the highest delays in all the cases and reauthentication only provides low delays if we stay in the same domain.

Regarding the energy consumed by the different authentication methods, we can see that reauthentication reduces the power consumed by eliminating the need to perform most of the cryptographic operations. Preauthentication, on the other hand, not only does not reduce the power consumed, but it increases it by preauthenticating to all the neighbor networks when the MN is notified about their presence. Finally, the optimized preauthentication performs similarly to reauthentication, due to the optimal combination of preauthentication

and reauthentication.

VI. Conclusions

In this paper we analyzed the performance of the authentication optimizations during handovers. We showed that optimizing the handover mechanisms while requiring the execution of a full authentication protocol makes the authentication the most important problem in our goal of achieving seamless handovers. Similarly, optimizing only the authentication process only reduces partially the problem and the current optimization proposals require information that may not be available for mobile nodes.

By using IEEE 802.21 mechanisms and services we managed to optimize the handover process as a whole, enabling the timely delivery of information to the mobile node, which was then capable or making accurate decisions about the handover. Furthermore, we showed how the use of the Media Independent Information Service makes it possible to integrate all of the authentication optimizations reviewed and to take advantage of their strengths.

We can see how the optimized proposal performs always as the better of the different alternatives by carefully selecting the adequate authentication scheme to use based on the information provided by the MIIS.

References

[1] P. Bellavista, A. Corradi and C. Giannelli, Adaptive Buffering-Based on Handoff Prediction for WirelessInternet Continuous Services. High Performance Computing and Communications, 2005. HPCC 2005. LNCS Vol. 3726, pages 1024–1032, Sorrento, Italy. Sep. 2005.

[2] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson and H. Levkowetz, Extensible Authentication Protocol (EAP), Internet Draft, RFC 3748. June 2004.

[3] T. Clancy and H. Tschofenig, EAP Generalized Pre-Shared Key (EAP-GPSK) Method, Internet Draft. July 2008.

[4] S. Deering and R. Hinden, Internet protocol, version 6 (ipv6) specification, Draft Standard, RFC 2460. December 1998.

[5] P. Funk and S. Blake-Wilson, EAP Tunneled TLS Authentication Protocol Version 1 (EAP-TTLSv1), Internet Draft. March 2006.

[6] Draft IEEE 802.21-2008. IEEE standard for local and metropolitan area networks-part 21: Media independent handover services. June 2008.

[7] IEEE std 802.16e-2006. IEEE standard for local and metropolitan area networks-part 16: Air interface for fixed and mobile broadband wireless access systems. Amendment 2: Physical and medium access control layers for combined fixed and mobile operation in licensed bands and corrigendum 1. Feb. 2006.

[8] IEEE std 802.11r-2008. IEEE standard for local and metropolitan area networks-part 11: Wireless lan medium access control (mac) and physical layer (PHY) specifications. Amendment 2: Fast BSS transition. Jul. 2008.

[9] C. Kaufman, Internet Key Exchange (IKEv2) Protocol, Proposed Standard, RFC 4306. December 2005.

[10] R. Koodli, Mobile IPv6 Fast Handovers, Proposed Standard, RFC 5268. June 2008.

[11] V. Narayan and L. Doneti, EAP Extensions for EAP Re-authentication Protocol (ERP), Proposed Standard, RFC 5296. August 2008.

[12] National Institute of Standards and Technology, Seamless and Secure Mobility project. http://www.antd.nist.gov/seamlessandsecure.shtml Retrieved on August 2008.

[13] Ns-2 simulator, http://nsnam.isi.edu/nsnam/index.php/Main_Page Retrieved on August 2008.

[14] Y. Ohba, EAP Preauthentication Problem Statement, Internet Draft. February 2008.

[15] S. Thomson, T. Narten and T. Jinmei, IPv6 stateless address autoconfiguration, Draft Standard, RFC 4862. September 2007.

[16] S. J. Yoo, D. Cypher and N. Golmie, LMS predictive link triggering for seamless handovers in heterogeneous wireless networks. Military Communications Conference, 2007. MILCOM 2007. IEEE, pages 1–7, Orlando, FL, USA. Oct. 2007.