Improving Security Information Gathering with IEEE 802.21 to Optimize Handover Performance

Antonio Izquierdo
National Institute of Standards and Technology
100 Bureau Dr, Stop 8920
Gaithersburg, MD, 20899-8920, USA
aizquier@nist.gov

Nada T. Golmie
National Institute of Standards and Technology
100 Bureau Dr, Stop 8920
Gaithersburg, MD, 20899-8920, USA
nada.golmie@nist.gov

ABSTRACT

In mobile networks, authentication is a time-consuming operation that needs to be shortened in order to provide seamless handovers. Furthermore, the time required for negotiating security parameters and obtaining security policies increases the importance of the authentication performance during handovers. Many optimizations have been proposed for different authentication mechanisms in different layers. However, they fail to provide means to learn in advance security capabilities and policies in candidate networks, and thus do not reduce the chance of connecting to potentially incompatible target networks. In this paper we use the information capabilities provided by IEEE 802.21 and propose an extension to current network selection algorithms that takes into account security parameters and policies to optimize the handover performance and reduce the negotiation delay.

Categories and Subject Descriptors

B.8.2 [**Performance and Reliability**]: Performance Analysis and Design Aids; E.3 [**Data Encryption**]: Standards

General Terms

Security, Standardization, Performance

Keywords

Handover, IEEE 802.21, Security configuration

1. INTRODUCTION

In recent years mobile and wireless technologies have experienced a significant growth, both of new capabilities and widespread availability. Seen as a low cost investment means for attracting new customers and offering new services, more often wireless networks are deployed by service providers, public transportation authorities, small business and franchises, etc. Furthermore, private wireless networks are deployed within organizations to improve flexibility, facilitate relocation and reduce the cabling required to service all employees that require network access.

In turn, further research on these wireless networks has provided new and better capabilities, that include, among others, bandwidth similar to that of wired technologies, larger coverage areas, increased reliability, more secure protection mechanisms and coexistence with other technologies.

The next challenge that industry and the research community have to tackle is user mobility: As network devices move from the coverage area of a network to that of a different network, mechanisms to facilitate this transition have to be provided. As a response to this need for seamless mobility some of the wireless technologies already provide mechanisms and techniques to ease the transition from one network to another, but we are still faced with several important issues, namely the mobility across heterogeneous wireless networks, and the integration of the mobility optimizations and techniques used in different layers of the network stack.

This last issue is specially interesting when optimizing security mechanisms. Traditionally, the security of a network connection is achieved by using different mechanisms in different layers that, independently, protect the communication against different types of attacks. These security functionalities were isolated from one another, so the security process at the network layer did not interact in any way with the mechanisms in place for the network access or transport layers. In this way, the different security measures in place acted as a single multilayered security mechanism. Currently there are efforts within IETF to integrate these security mechanisms, such as [4]; however currently that work only provides some of the mechanisms required to perform secure seamless handovers (e.g., a capability announcement mechanism is not provided).

However, the delay introduced by these mechanisms is quite significant, especially when all of them have to be processed one after another (as is the case during a network entry). While this delay is acceptable for a first network entry (as there is still no application data being transmitted), during a handover (HO) long delays mean large traffic disruptions. In order to achieve seamless handovers the security mechanisms need to be optimized for fast network switching, and should be capable of exchanging information with other network layers to ensure proper timing on all the operations.

These improvements made to the security mechanisms are specific to the security mechanisms considered. For example, it is not possible to transfer the security context from the old Point of Attachment (PoA) to the new PoA, due to the possibility of a security breach being propagated from one network to another.

MSWiM'09, October 26–29, 2009, Tenerife, Canary Islands, Spain.
Copyright 2009 ACM 978-1-60558-616-9/09/10 ...$10.00.

Additionally, the security negotiation introduces further complexity, as only in the negotiation of the security parameters the Mobile Node (MN) and the target PoA or Access Router (AR) are involved in a negotiation of parameters that may lead to a disconnection (if they cannot reach an agreement on the security policy to use). In general, the security parameters that a network accepts are made available to all potential nodes of the network (e.g., via open broadcast messages) only at the MAC layer, and even so, sometimes this information is not enough. For example, when using the Extensible Authentication Protocol (EAP, [3]), the specific EAP methods being supported are not advertised. As we can see, in many cases the MN initiates the connection with a network that may end up not using, based on the security policies in use.

In this paper we focus on the delay the security processing introduces in a handover. We consider the delays caused by the execution of security protocols in layers 2 and 3 and we also consider the effects of the negotiation of the security parameters, including when this negotiation results in the rejection of the candidate network (thus, forcing the mobile node to restart the handover process). We analyze what is needed to prevent these delays, and propose solutions based on mechanisms and services defined by the IEEE 802.21 standard.

Furthermore, we propose an extension to be added to existing network selection algorithms, that makes use of the solution proposed and prevents the mobile node from selecting a target network with incompatible security policies. This extension is defined as two separate modules, so that it can be easily adopted by the existing network selection algorithms.

The remainder of the paper is organized as follows. In Section 2 we review related work in the handover optimization area. Section 3 analyzes a handover, with a special interest on the role of security mechanisms both in layers 2 and 3. In Section 4 we introduce our extensions to target selection algorithms, and in Section 5 we show the simulation results obtained with the application of these extensions. Finally, in Section 6 we present our conclusions.

2. RELATED WORK

The research community has been very active in recent years in reducing the disruptive effects of network handovers by proposing optimizations to existing mechanisms, new mechanisms that add functionality to existing procedures, optimizations to existing mechanisms and external services and protocols that help the transition from one network to another.

Among these works, there are several proposals that focus on security signaling: In [10], Kassab et al use mathematical models to evaluate the performance, in terms of signaling overhead, of different reauthentication methods proposed for 802.11 networks. Similarly, Boulmalf et al ([5]) study the impact of security parameters in data and voice traffic in 802.11 networks without handovers, in order to provide common grounds for subsequent research.

Proposals related to layer 2 authentication are divided in two different groups: the proposals that are based on reusing the existing authentication information to accelerate the network entry (reauthentication), and the proposals that try to perform the authentication before the handover happens (preauthentication). In the first group, the most relevant contributions are based on EAP ([3]), like those of Nakhjiri et al ([12]), and the IETF study group HOKEY, which resulted in the standardization of EAP extensions in [13]. As for contributions based on preauthentication schemes, the most significant work has been done by Dutta et al ([6]) in the MOBOPTS working group of the Internet Research Task Force (IRTF).

As we move to layer 3, we find proposals of new authentication protocols that perform optimally in certain handover scenarios, such as the authentication protocol designed by Kang et al in [9], or the registration scheme presented by Kafle et al in [8]. Also, some works were focused on the analysis of the proposed solutions, as we find in [7], where Ghebregziabher et al provide a security analysis of flow-based handover methods.

Additionally, some other works have focused on the addition of external services and architectures to support seamless handovers across several layers of the networking stack. For example, the IEEE 802.21 draft standard ([2]) proposes several services and mechanisms that are aimed to support the mobile node and the network in the handover process.

As we can see, none of these contributions consider the increased delays caused by network disconnections due to incompatible security policies. As the next section describes, this may happen both in layer 2 and layer 3, and may render useless all the efforts to achieve seamless handovers.

3. ANALYSING HANDOVERS

In this section we present an analysis of a handover, with special focus on the security mechanisms and protocols involved in the process. We review the signaling and the different steps performed to accomplish the mobility from one network to another. In our study we consider handovers that use Mobile IPv6 Fast Handovers (FMIPv6, [11]) and IEEE 802.21 to support the handover. Also, we make use of the predictive mechanism described in [15] for the 802.21 link triggers. This mechanism is based on the MN's knowledge of the time required to prepare and perform a handover, so that it can periodically decide whether it has to start a handover or not. In order for this estimation to be accurate, the MN needs to know the time required to execute all of the steps described below. As this may require information that is not available using L2 or L3 mechanisms, the MN will use the IEEE 802.21 Media Independent Information Server (MIIS) to gather the information required. This allows the MN to update the time required for each step and for the whole handover whenever needed (e.g., a new candidate network is detected).

In Figure 1 we show all the steps performed during a predictive handover. In this figure the active scanning messages are represented with dashed lines, and exchanges that may require more than a request / response message pair are pictured as wide double-headed arrows.

As mentioned earlier, the MN constantly monitors the network conditions and makes estimations on those conditions in the future. When it predicts that in the time it takes to prepare and execute a handover the conditions will degrade below acceptable limits, a Link Going Down indication is triggered.

Upon reception of this indication, the mobile node performs the network discovery process to detect candidate networks. As we can see in this figure, this discovery may be performed by using the scanning procedures of the different

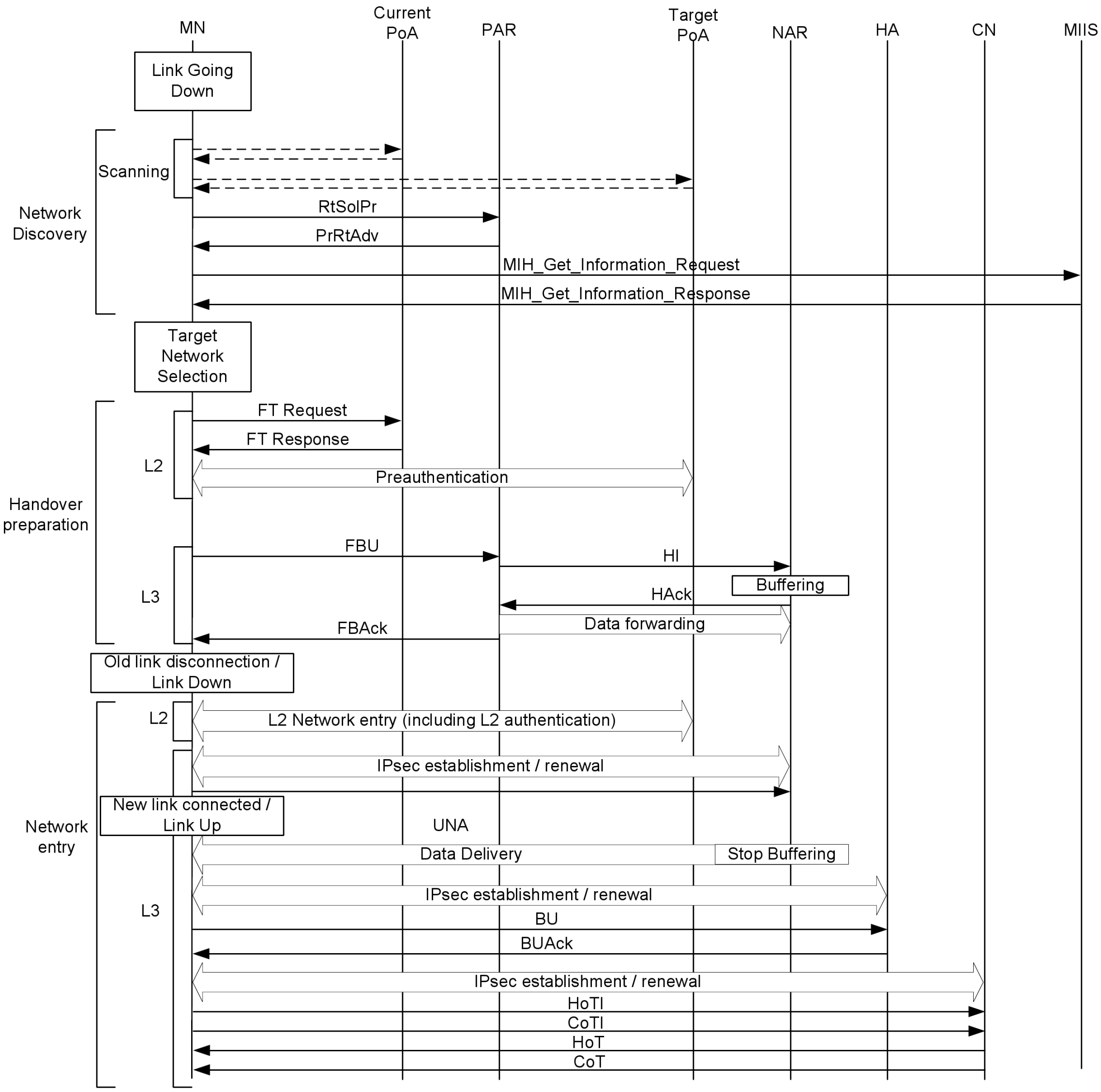

Figure 1: Handover messages.

interfaces, by requesting information at the IP level, and by querying the MIIS. These techniques can be used simultaneously, as they complement each other: while the scanning will yield up-to-date results that may be obsolete in the MIIS, the MIIS can provide extended information about each network not available through the scanning. Also it is important to note that, depending on the policy of the MN, this discovery phase may be performed constantly as a background task, instead of waiting for the Link Going Down trigger. In this case, when a Link Going Down indication is received, if the MN considers that the information gathered is fresh enough, it can omit the discovery phase.

When the discovery phase concludes, the MN chooses the target network from all of the candidate networks available. This selection is made based on the MN policy, which may consider a number of factors, like the signal strength of the target PoA, the security capabilities, the network operator, etc.

Once the target network is selected, the MN initiates the preparation of the handover. These steps can be performed in parallel, although in the figure they are shown sequentially for clarity. At the IP level, this preparation involves the FMIPv6 signaling to notify the Previous Access Router (PAR) and the New Access Router (NAR) of the handover, and the computation of the MN's address in the target network. Also, if the MN has to establish a new IPsec Security Association (SA) with the NAR, it may do so at this point, so that during the network entry it can use MOBIKE to reduce the latency of the process.

Regarding the L2 preparation, the MN may notify the current PoA of the handover to the target network, in order to use technology-specific optimizations (e.g., those defined in IEEE 802.16e). Also, if preauthentication is supported in the target network, the MN will perform it now.

Upon completion of these preparations, the data is forwarded from the PAR to the NAR where it was being buffered while the MN was entering the new network. This entry involves the L2 entry (including the L2 authentication signaling), and the L3 network attachment involves the establishment or renewal of an IPsec SA with the NAR and the signaling to forward the buffered messages. When the SA with the NAR is established and the MN has send an Unsolicited Neighbor Advertisement (UNA) to the NAR, the MN is attached to the new network and sends the Link Up indication. However, there are still some actions to perform to finalize the FMIPv6 protocol: the MN notifies the Home Agent (HA) of the new address, and optionally, performs the route optimization process with the Corresponding Nodes (CNs). These exchanges with the HA and the different CNs may involve the establishment or renewal of IPsec SAs, depending on the security policies and whether MOBIKE is supported or not. In Figure 1 we show the case where all the nodes require an IPsec SA in order to exchange IP control messages.

4. EXTENDING THE TARGET NETWORK SELECTION

In this section we present two modular extensions to network selection algorithms that prevent the problems resulting from incompatible security policies, and provide more accurate security signaling delay estimations, which, in turn, result in more accurate handover delay estimations. The first module is used to avoid the selection of networks that have incompatible security policies, while the second module limits the late failure of predictive optimizations.

In order for these extensions to work, the MN has to gather information regarding the security capabilities, requirements and policies of the candidate networks. We use the 802.21 MIIS to provide this information, as it is intended to include extended cross-layer information about different networks.

4.1 Security policy filtering

This extension adds two additional steps in the network selection process. The first of these steps involves the gathering of security-related information about the candidate networks discovered. As we explained previously, some of this information will be available through the discovery process itself (e.g., the authentication methods supported in L2). However, other pieces of information, such as L3 security policies, optimizations supported, etc. will have to be acquired by other means. In our case, we use the 802.21 MIIS to provide this information.

Once this information is gathered, the second step is performed: to filter out all candidate networks with incompatible security policies. The mechanism used to carry out this policy-matching process is out of the scope of this paper, as it will depend on implementation decisions (e.g., whether the MN has a single policy for all the L2 technologies or a different policy per technology). With this step we make sure that only networks with acceptable security policies are chosen by the network selection process, thus eliminating the possibility of initiating the connection to a network that has to be discarded later.

Furthermore, by gathering the information about the security policies and optimizations, it is possible to feed this information to the network selection algorithm, so that it can use the information, combined with the capabilities of the MN (e.g., the cryptographic delays with different algorithms) to better select the optimal candidate network.

This use of security policy matching techniques as a realtime mechanism to prevent disruption is novel in the literature and the industry. Moreover, this is the only proposal that can prevent the rejection of a target network during handovers due to the security policies in use (regardless of the technologies and security mechanisms used), while dynamically adapting to the MN's movement across networks and domains. As the cost (in terms of disruption time and packet loss) of these rejections is very high, the policy-filtering extension is a key component to achieve seamless handovers.

4.2 Optimization verification

The second of our extensions is to be executed after the target network has been selected. With this extension, the different optimizations of the security processes to be performed during the handover are evaluated and any action that the MN is required to perform before disconnecting is carried out and the result of this operation saved. For example, if the L2 of the target network supports preauthentication, the MN will proceed with all the preauthentication exchange, and save the result of this operation. However, if the L2 supports reauthentication and the MN can use it, no action is required until the network entry.

Upon the identification of the optimizations supported, and the successful preparation for them, the time required during the network entry for the authentication (both L2 and L3) is updated. The L2 authentication time (t_{authL2}) will be the time required for performing either a full authentication, a reauthentication or a preauthentication. The L3 authentication time will be the sum of the time required to establish the IPsec SAs with the NAR ($t_{IPsecNAR}$) and all the other required nodes (t_{IPsec_i}), considering whether it is possible to use MOBIKE or not. Finally, the total time required for the authentication processes (t_{auth}) is computed. This is the time that the prediction mechanism will use to estimate the start of a handover.

This process is performed in parallel for all the steps in which a security procedure is required: the PoA in L2, the NAR, Home Agent and corresponding nodes in L3. As soon as one of these operations fails, the handover to that target network is considered risky and a new target is selected from the list of candidate networks. The reason for considering the network risky and discarding it as a candidate even if what failed is not an essential security process for the network entry (e.g., the IPsec SA needed to perform Route Optimization in a Mobile IPv6 capable network), is that some of the information we gathered about the network was not correct. As there is mismatched information, the network is considered unreliable, and thus, excluded from the list of candidate networks.

Also it is worth noting that there may be some decisions and steps that do not affect the timing of the thresholds, but need to be performed to ensure that some optimizations will work during the handover. For example, if an optimization requires certain parameters to be exchanged prior to the handover (e.g., MOBIKE requires the MN to inform the CN about the future address), the first time we consider this optimization the MN will send and receive the required messages. However, during further analysis of this optimization in this network, that exchange is not necessary. In both cases, the expected time to perform the entry will be the same, regardless of whether the exchange took place or not.

In this case, the optimization-assurance extension provides a novel solution to reduce the uncertainty about whether the expected security optimizations will work as expected during the handover or not. This extension allows the MN to choose the available optimization that better suits its policies, and to consider the possibility of an error in the optimization process before the actual handover. As a result, the MN can select a different set of optimizations, or even a different target network, dynamically adjust the handover parameters to suit the new selection.

Furthermore, this extension provides a means to accurately predict the authentication delay during the handover. This is important as many handover optimization mechanisms rely on this information being available. Without our extension, the MN has to use information from previous handovers (which may not be applicable to the next one) or estimations. This extension manages to provide accurate delay information about each authentication phase, while also adapting dynamically to changes in the target network and the optimizations supported.

4.3 Using the extensions

As we can see, the proposed extensions require time to be completed, so modifications have to be done to the network selection process in order to prevent the disconnection of the MN from the old network while still selecting the target network. Although the simplest solution would be to update the thresholds at which the MN initiates the discovery procedure as needed, the integration with proposals that use periodic evaluation of the required handover time is more interesting. In these proposals (e.g., [15]), the MN periodically computes the required handover time, and adjusts the 802.21 link triggers accordingly. However, this periodic operation does not mean the the MN has to scan for candidate networks each time, as the information may come from other sources such as the 802.21 Information Server or broadcast announcements of neighbor capabilities. Our extensions could be easily integrated in this architecture, by including the discovery, filtering selection and testing in each of the iterations. The delay for the whole process would be reduced after the first iteration, as the predictive optimizations would only have to be performed again in case the target network selected was different from that of the previous iteration.

The total time required to perform the operations of the extensions is small, regardless of the density of neighbor networks: The policy-filtering extension requires several comparison of methods and / or polices, which can be done in parallel, and the operations in the optimization assurance extension only have to be performed the first time a neighbor network is selected as potential candidate, and even in that case, many of the operations can be parallelized. Thus, the overhead introduced in the overall network selection process is very small.

In Figure 2 we present an example of the use of these extensions with a network selection algorithm, with the details of the optimization verification extension shown in Algorithm 1. This flowchart shows the complete network selection process, with both extensions integrated together with the network selection algorithm described in [15], in an environment where networks support L2 reauthentication and preauthentication, and L3 MOBIKE. Of course, the application and results would be similar with other L2 and L3 optimizations. When the process is finished for a target network, the time required during the handover to perform each authentication phase is computed, and the required handover time is dynamically adjusted to reflect these changes.

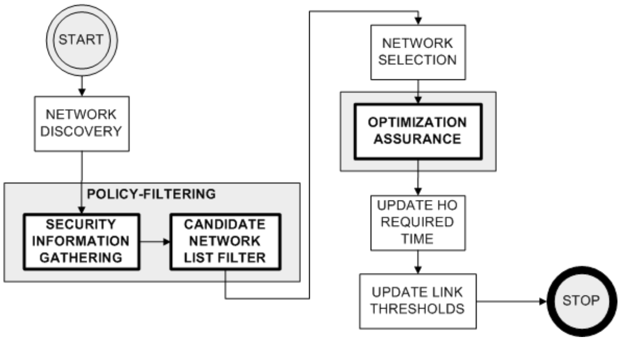

Figure 2: Network selection process with the proposed extensions.

While we showed the integration of the proposed extensions with a specific network selection algorithm, they can be used with any other mechanism and useful to assess the security delays incurred during a handover.

The performance of this schema is shown in the next section, where we simulate several handovers under different conditions to evaluate these extensions.

5. SIMULATION RESULTS

In this section we present the performance results obtained with our proposal, and compare them with the results when our proposal is not used. In order to obtain these results we simulated handovers between networks using the network simulator NS-2 ([1]) with the 802.21 extensions developed at NIST ([14]).

We first describe the simulation environment and conditions, and then we explore the results obtained in three different experiments.

5.1 Simulation environment

In order to perform the different tests described followingly, we used the NS-2 simulator with the 802.21 extensions from NIST ([14]) to provide the required functionality.

The network topology used in the tests is shown in Figure 3. It is composed of seven wireless networks using IEEE 802.11, where the Access Points also act as Access Routers. Each network is served by a single node that performs as Point of Attachment (PoA-0, PoA-1, etc.) and as Access Router (AR-0, AR-1, etc.). All these networks, except the initial one (served by PoA-0 / AR-0), belong to the same administrative domain, which may be the same or not as the domain of PoA-0 (depending on each test). AR-0 is the MN's Home Agent.

In this environment, the MN will move as indicated in the Figure 3. During that movement, the MN monitors the network conditions and estimates whether a handover is necessary or not. When the MN received the Link Going Down indication, it can discover all the networks served by all the PoAs, with PoA-1 being the one with the strongest signal. At this point the process described in Section 3 starts. De-

```
Input: Candidate network
Output: HO required time for security
/* Prepare L2 */;
if Same network domain AND reauthentication supported then
    Expect L2 reauthentication ;
    $t_{authL2} = t_{reauth}$;
else
    Start L2 preauthentication;
    $t_{authL2} = t_{preauth}$;
end
if authentication error then
    Discard candidate network;
else
    HO security required time = $t_{authL2}$;
    /* Prepare L3 */;
    if NAR supports MOBIKE then
        Establish IPsec with NAR with MOBIKE support;
        $t_{IPsecNAR} = t_{MOBIKE}$;
    else
        $t_{IPsecNAR} = t_{IPsec}$;
    end
    HO security required time += $t_{IPsecNAR}$;
    foreach L3 node in the mobility protocol do
        if Node supports MOBIKE then
            if UPDATE_ADDRESS required then
                Perform UPDATE_SA_ADDRESSES;
            end
            $t_{authL3} = t_{MOBIKE}$ ;
        else
            $t_{authL3} = t_{IPsec}$;
        end
        if IPsec error OR MOBIKE error then
            Discard candidate network;
            break;
        else
            HO security required time +=$t_{authL3}$;
        end
    end
end
```

Algorithm 1: Optimization assurance detailed algorithm.

pending on the experiment, this attachment may fail, in which case the MN will start the discovery process again.

These networks are 802.21 enabled, and there is a common Information Server that provides information about all of them. In our case, the information provided by the MIIS regards the security policies and configurations, and the optimization capabilities of each of the networks.

We also show in the topology the location of the CN, which maintains a data traffic flow with the Mobile Node while it handovers from one network to another.

Finally, the Mobile Node starts the simulation attached to the Access Point 0 (PoA-0), and moves towards PoA-1, until it exits the coverage area of its old network, and has to handover to a new one. At this point the MN will detect all the PoAs, with PoA-1 having a better signal quality.

For this study we use IPv6 stateless address autoconfiguration and FMIPv6, in both its predictive and reactive modes. Periodic Router Advertisement (RA) messages are sent every 2 seconds, and the lifetime of that information is 18 seconds.

The traffic used in the simulation is a Constant Bit Rate (CBR) traffic transmitted over TCP with a frequency of 20 packets per second and a packet size of 1000 bytes. This traffic is sent from the CN to the MN.

The authentication method supported by the MN is EAP-based, both for L2 and IPsec authentications. This will require the PoA (or the IPsec responder) to contact the EAP server in the network, which will add additional delay. The EAP methods used are EAP-Generalized Pre-Shared Key (EAP-GPSK) and EAP-Tunneled TLS v0 with MD5 authentication (EAP-TTLSv0-MD5) (that is, EAP-TTLSv0 to establish a cryptographic tunnel, and an MD5 challenge-response inside the tunnel to finalize the authentication). EAP-GPSK is a fast, symmetric cryptography-based authentication method, while EAP-TTLSv0-MD5 is a complex method that uses asymmetric cryptography to establish the TLS tunnel. By using these two different methods we provide guidelines about the performance of these two different families of EAP methods, along with boundaries for their performance, so that, even if actual performance results are different (as they heavily depend on the hardware platform used), the trends and relative results would be similar to those presented here.

Regarding the optimizations considered in these simulations, we test the performance when using L2 reauthentication and preauthentication, and L3 MOBIKE integrated with FMIPv6 as said previously. We consider that both the Home Agent and the CN support MOBIKE, and both of them have security policies compatible with that of the MN.

In this environment, we define the following metrics to study the performance of the handovers:

- *L2 handover delay* is the time between when the L2 initiates the handover process with the network discovery, until the MN is capable of sending L2 data packets in the new network. In the event that the network entry fails (either at layer 2 or 3), we consider the L2 handover delay to be the time between the initiation of the handover to the first target network, and the successful L2 attachment to the final network.

- *L2 authentication signaling delay* is the time required to signal all the messages needed to perform an L2 authentication during the network entry, since the first message is sent until the acknowledgment for the last message is received.

- *L3 handover delay* is the time between the L3 starts the handover operations in the new network until the data traffic is restored. In the event that the network entry does not succeed, we consider the L3 handover delay to be the time between the initiation of the L3 handover operations in the first target network, and the restoration of the data traffic.

- *IPsec delay* is the time required to establish a new IPsec SA or reconfigure an existing one during a network entry.

As the L2 authentication signaling is part of the L2 network entry, the L2 handover delay is the sum of the L2 authentication signaling delay and the time required to carry out other L2 operations during the network entry.

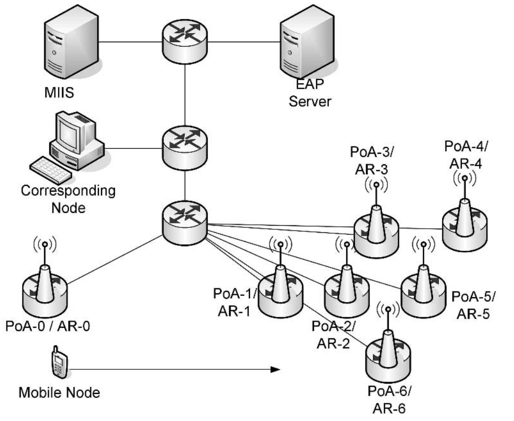

Figure 3: Network topology used in the simulations.

Similarly, the L3 handover delay includes the time required to perform the L3 mobility signaling (depending on the protocol used), and the establishment or reconfiguration of the IPsec SAs. In a handover that uses FMIPv6, such as the one shown in Figure 1, there are three different IPsec SAs to establish (each one with its own delay). In this case the L3 handover delay is the sum of the IPsec delay with the NAR, the IPsec delay with the HA, the IPsec delay with the CNs, the transmission delay for the UNA, the transmission delay for all the buffered packets, the Binding Update message exchange delay and the Route Optimization exchange delay.

In the following subsections we analyze the performance of our proposed network selection extensions, as compared to the same network selection algorithm without our extensions. We compare the cases in which the MN can handover to the network served by PoA 1, to make sure that our extensions do not degrade the performance when the predictions are correct, and then consider the cases in which that network does not use compatible security policies (at the different layers), so the MN is forced to handover to the network of PoA 2.

5.2 Experiment 1

First, we consider the case in which Network 1 is an optimal target network, meaning that it supports handover and authentication optimizations, the security policies are acceptable by the MN and the handover succeeds. In this scenario the MN can use any optimization that it supports, and our extensions will provide the least improvement. Thus, this experiment serves to evaluate the overhead that the extensions may introduce in optimal scenarios.

In this case, the MN will be able to use L2 reauthentication or preauthentication, and the IPsec SAs with the HA and the CN can use MOBIKE to reduce the L3 handover delay. In order to compare the optimal case for both reauthentication and preauthentication, the MN's Link Going Down threshold has been configured so that, when triggered, the MN has enough time to perform the preauthentication with all the required networks. However, we should note that this may not always be the case, as the preauthentication signaling may be very time consuming, specially in scenarios with several overlapping networks. In these scenarios, as the MN moves, the target network of choice may change quickly, so the MN may not have time to complete the preauthentication process.

In Table 1 we show the handover delay for both the L2 and the L3, when the MN makes its decision based on the signal strength and when it uses our proposed extensions to the target selection process. We also provide the delays when no L2 optimization is used and the MN has to perform a full authentication. These values provide a reference of the improvements introduced by the authentication, and they also define the worst case scenario.

As we can see, when the target network chosen by the MN based on signal parameters only is an optimal election, using our extensions does not introduce any penalty in the handover.

5.3 Experiment 2

In this experiment we consider the case in which Network 1 does not support reauthentication, preauthentication nor MOBIKE, but all the other networks support L2 reauthentication and MOBIKE. In this situation, if the MN bases its target network selection on the signal strength alone, it will choose to handover to Network 1, which will require a long handover process. However, if the MN uses our proposed extensions and considers the availability of security optimizations as another factor in the selection algorithm, it will choose to connect to Network 2 (which supports optimizations and provides good signal quality).

The results of this experiment are shown in Table 2, where the handover and authentication delays for each network layer are shown. We see that when the MN does not use the proposed extensions and chooses the target network based only on the signal strength, it has to perform a full L2 authentication and establish a new IPsec SA with the NAR. This leads to handover delays that vary from 0.9 seconds to 2 seconds in L2, and from 2.8 seconds to 5 seconds in L3, depending on the EAP method used. In both cases, the total handover delay (about 3.67 seconds when using GPSK and 7.09 seconds if we use TTLSv0-MD5) is unacceptable for many applications.

As we can see, by using our extensions the MN was able to always choose a target network that supported authentication optimizations during the handover, thus reducing significantly the required handover time both in L2 and L3. Using this mechanism the total handover delay was 0.77 seconds.

Furthermore, by selecting a target network that supported both reauthentication and MOBIKE the MN managed to prepare a handover in which the security signaling in L2 and L3 is completely independent of the authentication methods used. This is very important for the prediction mechanisms, as the authentication signaling delay during the network entry will be the same, regardless of the policies of the target network.

5.4 Experiment 3

In this final experiment we configure the network so that the security policies in Network 1 are unacceptable by the MN, which will force the MN using the signal-based network selection to choose a different target network. However, if the MN uses our extensions, it will learn this situation in advance and filter out Network 1 from the list of candidate networks. All the networks support L2 and L3 authentication optimizations.

Table 1: Handover delay in experiment 1 (ms)

		L2 Handover			L3 Handover	
		Full Auth.	Reauth.	Preauth.	Without MOBIKE	With MOBIKE
Normal	GPSK	920.17	719.23	677.48	2755.32	51.02
	TTLSv0-MD5	2080.23	719.23	677.48	5008.65	51.02
Extended	GPSK	920.17	719.23	677.48	2755.32	51.02
	TTLSv0-MD5	2080.23	719.23	677.48	5008.65	51.02

Table 2: Handover and authentication signaling delays in experiment 2 (ms)

		Layer 2		Layer 3	
		Auth. signal. delay	L2 Handover delay	IPsec delay with NAR	L3 Handover delay
Normal	GPSK	194.33	920.17	2753.36	2755.32
	TTLSv0-MD5	1352.37	2080.23	5006.51	5008.66
Extended	GPSK	46.59	719.23	2.88	51.02
	TTLSv0-MD5	46.59	719.23	2.88	51.02

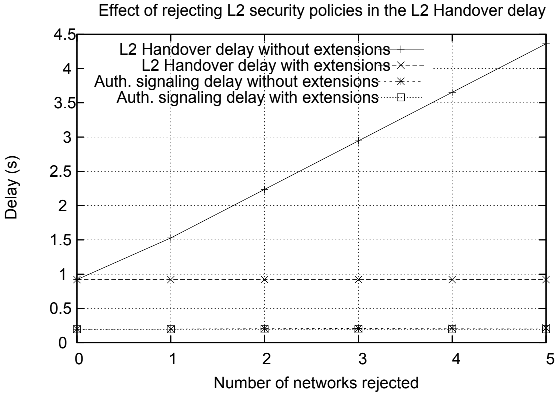

Figure 4: Effect of rejecting an L2 security configuration in the L2 handover delay.

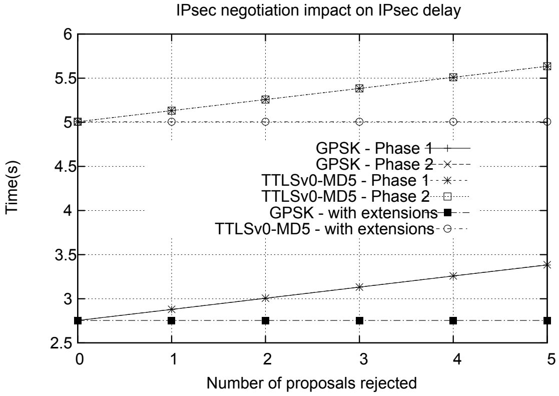

Figure 5: Variation of the IPsec delay with NAR-1 with the number of proposals negotiated.

In this experiment we will see how the negotiation of security parameters affects the handover, and how an unsuccessful negotiation (let it be in L2 or L3) leads to a network rejection and to the need for selecting a new target network.

The effects of the negotiation of the security policies are different depending on the layer on which they occur. In L2 the security parameters are advertised by the PoA, so the MN knows in advance that information. However, the EAP methods supported during the authentication are never announced, so this may be the cause of network rejections. As shown in Figure 4, the L2 handover delay and the L2 authentication signaling are affected by these negotiations. We also show in the same figure the performance of the L2 handover when using our extensions (even though there are no rejected security configurations), in order to better compare the difference of performance between both approaches. We can see that when a network is rejected due to the L2 security configuration, the authentication signaling does not increase significantly (as this rejection happens in the early stages of the authentication), but the L2 handover delay, however, experiences an important increase. This is due to the MN having to restart the network discovery procedures (scanning), selecting again a target network, and initiating the network entry procedure again.

In L3, however, the security policies are not advertised, so the possibility of the MN and the network having incompatible security policies is greater. Furthermore, as the L3 negotiation happens later in time than the L2 negotiation, the delay introduced when a network is rejected is much larger. Figure 5 shows the increase in the IPsec delay depending on the authentication method used, along with the performance offered by our solution (which, again, minimizes the negotiations because the MN knows in advance the methods supported). We can also see that, as long as the peers finally agree on a security proposal, the IPsec delay is affected the same way no matter if the security parameters are being negotiated for the authentication (Phase 1) or the SAs (Phase 2). However, this distinction is significant if the peers do not reach an agreement on the security configuration to use, as shown in Figure 6. In this Figure we see how the increase in the IPsec delay when none of the security proposals are acceptable by the MN and it has to search for a new network is higher if this rejection happens after the authentication, regardless of the authentication method used.

In Table 3 we show the effects on the L2 and L3 handover delays of the rejection of the target network. We consider the possibility of having a rejection at L2 or at L3. When the rejection happens at L2, the HO delay in this layer increases, but the L3 HO delay is the same as that of a handover that does not support optimizations. The reason for this is that by rejecting the network the MN moves to a NAR that was not expected, so no optimizations can be used.

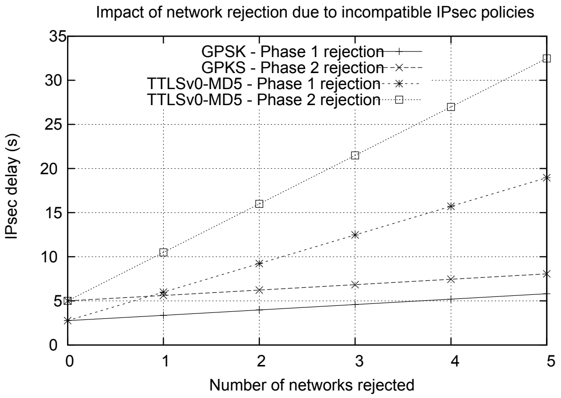

Figure 6: Impact of network rejection due to incompatible IPsec policies.

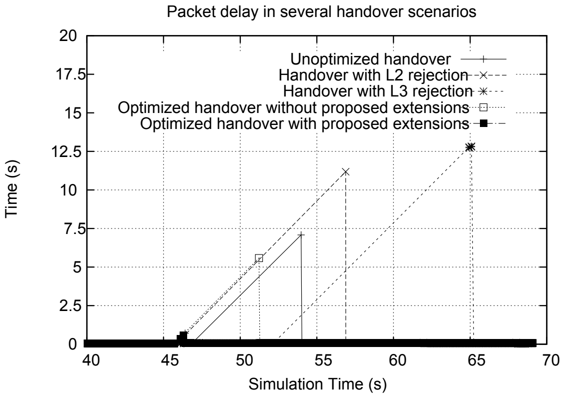

Figure 7: Packet delay in full handovers.

When the rejection happens at L3 the L2 handover delay is also affected, as after the rejection a new candidate network has to be selected, and the L2 network entry has to be performed again.

However, by using the proposed extensions the MN ruled out the networks with incompatible security policies, so it can optimize the handover, knowing in advance that the security policies are compatible.

An interesting result of the network rejection can be seen in Figure 7. In this figure we show the packet delay with different security configurations and MN's capabilities. We can see how the packet delay obtained during a handover without any optimization (*Unoptimized handover*) is higher than the packet delay obtained when using L2 and L3 optimizations, and much higher than the delay obtained by using the proposed extensions. However, if the predicted target network is rejected, the delays we obtain are much higher than the handover without optimizations, which serves as a metric of the real cost of a network rejection.

6. CONCLUSIONS

In this paper we proposed two extensions to the traditional network selection procedures, in order to optimize the security signaling during the handover. The policy-filtering extension filters the networks with incompatible security policies from the list of candidate networks, and the optimization-assurance extension makes sure that the optimizations expected will not fail during the handover. We showed that the delay introduced by the authentication signaling may be very high, as the security capabilities and policies are not always advertised. This may cause the MN to attempt to join a network with incompatible security policies or optimizations, thus forcing the disconnection from that network and starting again the network discovery and selection procedures. Furthermore, when this happens, all the handover optimizations that relied on some kind of predictions about the target network are rendered useless, and may even introduce some penalty in the application traffic.

By gathering additional security information from information services like the 802.21 Media Independent Information Service, it is possible to learn these capabilities in advance, filtering out the networks with incompatible policies. Additionally, by testing the predictive mechanisms before the handover is imminent, it is possible to detect any mismatch between the information gathered and the configuration, and prevent unexpected situations during the handover.

Our results show that our proposal does not introduce overhead on existing optimizations, and improves their performance when the additional information collected shows a better candidate network or optimization to use. By introducing these extensions in the existing network selection procedures it will be possible to combine the benefits of each of those procedures with the additional information and the optimization testing of our solution.

7. REFERENCES

[1] The Network Simulator NS-2, version 2.31. http://nsnam.isi.edu/nsnam/index.php/Main_Page.

[2] IEEE draft 802.21/d14. IEEE draft standard for local and metropolitan area networks - part 21: Media independent handover services. IEEE Draft 802.21/D14, Sept. 2008.

[3] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz. Extensible Authentication Protocol (EAP). RFC 3748 (Proposed Standard), June 2004. Updated by RFC 5247.

[4] B. Aboba, D. Simon, and P. Eronen. Extensible Authentication Protocol (EAP) Key Management Framework. RFC 5247 (Proposed Standard), Aug. 2008.

[5] M. Boulmalf, E. Barka, and A. Lakas. Analysis of the effect of security on data and voice traffic in wlan. *Computer Communications*, 30(11-12):2468–2477, 2007.

[6] A. Dutta, V. Fajardo, Y. Ohba, K. Taniuchi, and H. Schulzrinne. A framework of media-independent pre-authentication (mpa) for inter-domain handover optimization. Internet-Draft, July 2007.

[7] T. Ghebregzisabher, J. Puttonen, T. Hamalainen, and A. Viinikainen. Security analysis of flow-based fast handover method for mobile IPv6 networks. In *20th International Conference on Advanced Information Networking and Applications (AINA) 2006.*, volume 2, pages 849–853, Apr. 2006.

[8] V. P. Kafle, E. Kamioka, and S. Yamada. Extended correspondent registration scheme for reducing handover delay in mobile IPv6. In *7th International*

Table 3: Handover delay in experiment 3 (ms)

		L2 Handover delay	L3 Handover delay
Normal - L2 rejection	GPSK	1525.23	2755.32
	TTLSv0-MD5	2798.15	5008.66
Normal - L3 rejection	GPSK	2194.25	4356.36
	TTLSv0-MD5	6101.19	9168.66
Extended	GPSK	719.23	51.02
	TTLSv0-MD5	719.23	51.02

Conference on Mobile Data Management (MDM) 2006., pages 110–110, May 2006.

[9] H.-S. Kang and C.-S. Park. Authenticated fast handover scheme in the hierarchical mobile IPv6. In J.-K. Lee, O. Yi, and M. Yung, editors, *WISA*, volume 4298 of *Lecture Notes in Computer Science*, pages 211–224. Springer, 2006.

[10] M. Kassab, J. M. Bonnin, and A. Belghith. Fast and secure handover in WLANs: An evaluation of the signaling overhead. In *5th IEEE Consumer Communications and Networking Conference CCNC 2008.*, pages 770–775, Jan. 2008.

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

[12] M. Nakhjiri. Use of EAP-AKA, IETF hokey and AAA mechanisms to provide access and handover security and 3g-802.16m interworking. In *IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC) 2007.*, pages 1–5, Sept. 2007.

[13] V. Narayanan and L. Dondeti. EAP Extensions for EAP Re-authentication Protocol (ERP). RFC 5296 (Proposed Standard), Aug. 2008.

[14] NIST. Seamless and Secure Mobility project. http://www.antd.nist.gov/seamlessandsecure.shtml, Oct. 2008.

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