

An 802.1X-based Security Architecture for MIP

Rodolphe Marques, Hélio Araújo and André Zúquete

Abstract—The motivation of this paper is the need for security on Mobile IP (MIP) enabled networks. Nowadays, 802.11 networks rely on the 802.1X authentication protocol for authenticating mobile nodes requiring network access. MIP protocol could be used to enable those mobile nodes to access a network as their home network, without any IP configurations. However, many security issues confer some vulnerabilities for MIP enabled devices (mobility agent and users). Our approach enables MIP agents to get keys for message authentication purposes while (de)registering a mobile node in a network and provide trustworthy information about MIP agents that serve future roaming networks to mobile nodes. Furthermore, fast and secure MIP handovers are gracefully handled with a slight change in the MIP protocol. Finally, with our approach we achieve a functional, integrated security architecture handling both link layer and network layer mobility.

I. INTRODUCTION

Mobile IP (MIP [6]) is a long-standing and mature protocol designed to facilitate the physical mobility of IP endpoints attached to hosts. MIP requires the collaboration of several network entities, namely special hosts named *Home Agent (HA)* and *Foreign Agent (FA)*, for helping a *Mobile Node (MN)* to keep network connectivity without changing its network identity and context (IP address, network mask, domain names resolution context, etc.).

All MIP interactions with HAs and FAs must be properly secured in order to prevent these services from being improperly used by rogue clients (MN). On the other hand, a MIP client should be able to find and contact the correct HAs and FAs that should cooperate with it to support its mobility. Resuming, HAs and FAs should be able to authenticate MNs requests and MNs should be able to identify and authenticate the correct HAs and FAs.

Concerning security, MIP protocol messages contain *Authentication Extensions* that provide authentication via Message Authentication Codes (MACs) computed over the message contents with a secret key. Secret keys are kept within Mobility Security Associations (MSAs). A MSA is a security context, between a pair of nodes, which may be applied to MIP protocol messages exchanged between them. Each context indicates an authentication algorithm, a secret (shared key appropriate public/private key pair) and a replay protection style. However, is not in the scope of MIP to provide the means to efficiently derive and distribute the keys used to authenticate MIP messages.

This paper describes a security architecture for protecting MIP operations within a single security domain over a possibly large physical area (e.g. an University Campus). The architecture was built by extending another one [4], developed for protecting wireless, 802.11 link layer reassociations of MNs.

Here we describe how the original architecture was extended to manage MSAs for protecting MIP interactions and how MIP information is distributed in a protected way to MNs using 802.11 management frames.

The main advantage of our approach is that we are able to use the same security architecture, within a security domain, for protecting both link layer and network layer mobility control messages. Furthermore, by having an integrated management of both link layer and network layer mobility, we are able to anticipate traffic redirections to networks that will be visited by the MN, thus reducing the overall latency of handovers.

This paper is structured as follows: Section II briefly describes the security architecture developed for 802.11 link-layer mobility. Section III briefly describes the roaming process of a MN between networks revealing the MIP security issues that result of this mobility process. Section IV presents our contribution for integrating MIP with a local security architecture. Section V evaluates our contribution. Section VI presents the related work. Finally, Section VII concludes the paper.

II. ORIGINAL SECURITY ARCHITECTURE

The security architecture conceived for protecting MIP interactions is an extension of another one conceived for handling fast, secure handovers in 802.11 networks [4]. That security architecture follows the general reauthentication architecture and key hierarchy proposed by the HOKEY (HandOver KEYing) IETF Working Group [5], [7], which uses a local HOKEY service and key hierarchies starting in the 802.1X EMSK (Extended Master Session Key); the HOKEY service was nicknamed *Reauthentication Service (RS)*.

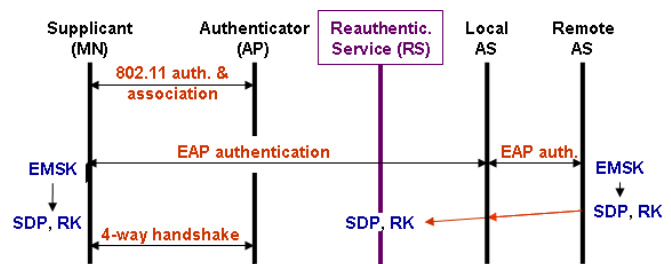


Fig. 1. Reauthentication Service: integration with the 802.1X architecture and secret material uploaded to it (SDP and RK) by the local AS upon a successful EAP-based authentication between the supplicant (MN) and the AS within 802.1X.

The RS was initially conceived for handling fast 802.1X reauthentications within 802.11 reassociations (see Fig. 1). Following the terminology of 802.11r, the RS is the enabler

of a **mobility domain**, which is formed by all Access Points (APs) that know how to reach and securely interact with the RS for handling MNs' reauthentication requests. The RS can be implemented in two different ways: (i) as part of a local 802.1X Authentication Service (AS); or (ii) as an independent, HOKEY server [5].

After an initial 802.1X authentication, APs use the RS instead of the AS for handling 802.1X reauthentication requests from MNs. Security associations are assumed to exist between all APs and the RS, similar to the ones that exist between APs and the local AS. These security associations are fundamental to (i) authenticate RS messages to APs and to (ii) enforce the confidentiality of keys provided by the RS to the APs.

For handling fast 802.1X reauthentications in a security domain managed by an same RS, MNs are identified by a unique identifier, the *STA Digital Pseudonym* (SDP). An SDP for a authenticated MN is computed during its first 802.1X authentication in the network and maintained by the RS. During the 802.1X authentication is also computed a *Reauthentication Key* (RK), also maintained by the RS. The RK will be used by the MN and the RS to authenticate each other in future 802.1X reauthentications.

The SDP and the RK are independently computed by the AS and the MN (802.1X supplicant) during the initial 802.1X authentication, and uploaded to the RS by the AS (see Fig. 1). Both values are computed with the PRF-X one-way function for key expansion [2] from a root key, the EMSK. According with [7], RK is a Domain Specific Root Key and SDP is a Domain Specific Usage Specific Root Key.

802.1X reauthentications are performed within new 802.11 authentication and reassociation protocols. The details of such protocols are irrelevant for this paper, except in one detail: the new 802.11 *Authentication Response* is authenticated with key material derived from RS. This means that such responses may carry authenticated information about the network where the AP is connected to, namely MIP-related information.

III. MIP SECURITY ISSUES

A MIP's MN has two addresses, a *home address* (HAddr) that it retains independently of its location, and a *care-of-address* (CoAddr), which is attributed to the MN, temporarily, assigned by the visited network.

When the MN moves to a foreign network, it finds the local FA by listening its broadcast advertisement messages and requests a CoAddr from the FA. This CoAddr is then registered in its HA with a *Registration Request* message. Hereafter, all data sent to the MN by *Corresponding Nodes* (CNs) arriving to the home network is tunneled by the HA to the MN's CoAddr, handled by the FA, which forwards it to the MN using its HAddr. On the contrary, packets sent by the MN are routed normally to destinations.

If the CN is also a MIP-enable host, a binding update may be sent to it containing the CoAddr of the destination, in order to optimize MIP routing delays. In this paper we will not consider this optimization, as it requires the existence of security relationships between the security domains of MNs

and CNs, something that is out of the scope of this paper. Therefore, we will only consider the case where all traffic directed to a MN passes through its HA. Note that this limitation is not dramatic for the mobility environment we are considering here (within a large network under the same security domain).

All this said, we have the following security issues for MIP:

- 1) Authentication of HAs and FAs. MNs must be able to authenticate network agents that are responsible for managing its local mobility, namely its HA and the FA of each visited network. The authentication goal is not to derive the *identity* of the agent, but instead to get convinced that it is not interacting with a *rogue* HA or FA.
- 2) HAs must authenticate the source origin of MIP requests sent by MNs. Otherwise, attackers could generate bogus *Registration Requests* specifying their own IP address as the CoAddr for a victim MN. Thereafter, all packets sent by a CN to the victim would be tunneled to the attacker.
- 3) HAs must validate the freshness of MIP requests sent by MNs. Otherwise, attackers could get copies of them and replay them at a latter time.
- 4) HAs must validate the correctness of the information they receive in *Registration Requests*. Namely, the HAddr provided in the Registration Request must be the one that was, and still is, assigned to the MN that issued the request. Otherwise, inside attackers (MNs capable of sending authenticated requests to their HA) could redirect traffic of other hosts connected to the home network.

Attacks against MIP are likely to create denial of service (DoS) scenarios to the MNs using it; victim MNs may stop getting data from CNs after such attacks. Furthermore, more dangerous attacks can be launched against MIP, such as man-in-the-middle attacks. In this case, attackers may redirect traffic by means of illegitimate MIP operations and relay traffic to the victim hosts in order to remain undetected.

MIP protocol messages can carry authentication codes for providing source authentication for recipients. Such authentication codes help to tackle the two first security issues. MIP messages can also carry timestamps or nonces to detect replaying, the third security issue. But MIP does not have any established mechanism to evaluate the correctness of MN's requests, the fourth security issue.

In this paper we only propose a security architecture to protect the current MIP protocol specification in a given operational scenario. Therefore, we do not address the correctness issue above referred, as it requires a deeper integration of MIP with IP binding policies and services, such as DHCP services [1].

IV. CONTRIBUTION

Our main goal was to reuse the security architecture presented in Section II to manage the security of a MIP environment. This way, we could have a clean, well-integrated

security architecture for managing both link layer and network layer mobility environments.

Our design goals were the following:

- 1) Use MIP without adding more complexity to an already complex protocol;
- 2) Define and distribute keys to authenticate messages exchanged during the MIP registration processes;
- 3) Proactively inform the MN about which MIP agent is serving a given access network, so that the MN can determine if it is about to roam to a different subnet or not;
- 4) Reduce as much as possible the latency of MIP handovers.

The RS is the most important entity of the authentication architecture presented in Section II, being responsible for deriving and distributing all keys required by 802.1X within reauthentications. We propose the use of the RS to distributed session keys to MNs and MIP agents to authenticate MN's messages, and vice-versa. The main assumption we make is that there are security associations between the RS and all the MIP agents (HAs and FAs) in the security domain of RS.

A. MIP authentication keys

To authenticate MIP messages, a set of Mobile Keys (MKs) was added to the 802.1X key hierarchy. Furthermore, the set of MK keys was divided in two subsets: one for authenticating MN requests (MK_{req} keys), and the other to authenticate MN responses (MK_{resp} keys). The keys in both sets derive from the RK and SDP values obtained during the initial MN's 802.1X authentication (cf. II) as follows:

$$MK_{req}(i) = \text{PRF-X}(\text{RK}, \text{SDP}, i, \text{"request"})$$

$$MK_{resp}(i) = \text{PRF-X}(\text{RK}, \text{SDP}, i, \text{"response"})$$

The MK keys can be derived independently by both MN and RS, because they both know RK.

We use MK_{req}(*i*) to authenticate MIP *Registration Request* and *Deregistration* messages. The *i* value used to compute MK_{req}(*i*) is a counter maintained by the RS and the MN, so that a fresh key is derived every time a new request occurs. HA and FA never have direct access to MK_{req}(*i*) keys, they only ask the RS to use them to validate requests. This way, malicious MIP agents cannot impersonate MIP requests of legitimate MNs.

Each time a MIP agent asks to validate a MIP request made by a MN, it receives a corresponding MK_{resp}(*i*) key for the same *i* if the request is valid. This key can then be used to authenticate the MIP agent reply to the MN.

MIP messages were kept unchanged; we only make use of the authentication extension provided, namely, the Mobile-Home Authentication Extension [6]. This tackles items 1 and 2 of our design goals.

B. MIP roaming awareness

We only use shared keys for authentication within MIP, and we need a different key for each pair of mutually authenticating entities. This means that we are not able to authenticate broadcast messages, such as FAs' *Router Advertisement* messages. However, we need to provide the MN some information for enabling it to know when it roamed to a different subnet.

To solve this roaming awareness problem, we added an extra field to the 802.11 *Authentication Response* message used on behalf of fast, 802.1X reauthentications. This extra field contains the IP address and network prefix of the MIP agent of the subnet the AP serves. As referred at the end of Section II, the *Authentication Response* is authenticated by the AP.

The MIP mobility awareness method works as follows:

- The MN performs an initial 802.1X authentication using a home AP.
- The MN gets an IP address for the current access network (its HAddr).
- The MN starts an 802.1X reauthentication protocol with the same AP and gets authenticated information about the network prefix and IP address of the local MIP agent (its HA).
- Each time the MN performs an 802.11 authentication in another AP, it receives authenticated information about the network prefix and IP address of the MIP agent serving the subnet handled by that AP. Since such authentications precede associations to APs, the MN knows what it needs to do regarding MIP roaming before actually moving to another AP.

This MIP awareness method fulfils item 3 of our design goals.

C. Reduction of MIP handover latency

As we saw above, a MN knows the MIP-related information of a network served by an AP before actually becoming associated to that AP. Thus, a MN can act as follows:

- Authenticate with a new AP *Y* while being associated with AP *X*. This authentication yields MIP-related information of the subnet served by *Y*.
- The MN decides to roam to AP *Y*. Consequently, it can start the registration of a CoAddr in the future network before actually moving into it.
- After actually roaming to AP *Y*, the MN may immediately start receiving data from CNs.

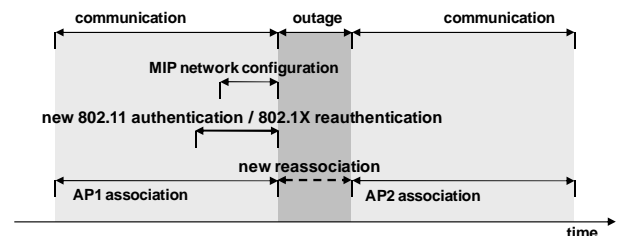


Fig. 2. Outage periods during a 802.11 and MIP handover by registering a CoAddr in the subnet of AP2 before actually reassociating from AP1 to AP2.

Concluding, we are able to completely eliminate the MIP network configuration latency by running CoAddr registration procedures before 802.11 reassociations (see Figure 2). This can be done with one special registration capability of MIP: to have multiple, simultaneous CoAddrs registered with the HA. When this happens, the HA tunnels a copy of packets destined to the MN to each one of the multiple CoAddrs. This way, we can have, for a short period of time, the packets sent simultaneously to the previous and the new CoAddrs. This period of time is the 802.11 reassociation time; afterwards, the MN can deregister its old CoAddr.

D. Protocol Description

This protocol description assumes that there are security associations between the RS and all the MIP agents (HAs and FAs) in the same security domain. It also assumes that the MN knows, before the handover decision: (i) if it is going to roam to a different subnet, (ii) if the new subnet has a FA, (iii) the IP address of the FA. Assuming that the MN is going to roam to a different subnet, there are two possible scenarios: (i) the target subnet has a FA or (ii) the target network has no FA. For lack of space, we will not describe this latter case.

Figure 3 shows the message exchange that happens when the MN roams to a subnet where a FA exists. The protocol works as follows:

- 1) After the 802.11 authentication, the MN knows that the target AP serves a different subnet, and also knows the IP address of its FA.
- 2) When the MN decides to roam to that subnet, it first sends an *Agent Solicitation* message to the future FA. This solicitation differs from a normal one because it uses the FA's unicast address, instead of a broadcast destination address. This must be done because we want this message to be sent before the association with the new AP, and, at this point, the MN does not belong to the subnet of the target AP. The *Agent Solicitation* message is authenticated with the key $MK_{req}(i)$.
- 3) After receiving an *Agent Solicitation* message from the MN, the FA will ask the RS to authenticate the message, and if successful the RS will send the FA the $MK_{resp}(i)$ so that the FA can authenticate its next responses.
- 4) The FA will then send an *Agent Advertisement*, once again differing from a normal *Agent Advertisement* message because the destination address field of this message will be the MN's HAddr. This message is now authenticated with the key $MK_{resp}(i)$.
- 5) After receiving the *Agent Advertisement* message, the MN will start the CoAddr registration process with its HA. This process is a normal MIP registration process, where we use the extensions to provide the MN's SDP to the HA. Hence, the MN sends a *Registration Request* message to its HA with its SDP and the Mobile-Home Authentication Extension calculated with the $MK_{req}(i)$.
- 6) The FA processes the *Registration Request* message, and if correct, it relays the message to the HA.

- 7) Upon receiving the *Registration Request*, the HA asks the RS to authenticate the message associated to that SDP (for a given i). If successful the RS will provide the HA with the $MK_{resp}(i)$ so that the HA can authenticate the response.
- 8) After receiving the $MK_{resp}(i)$, the HA processes the message. If correct, it sends a *Registration Reply* authenticated with the $MK_{resp}(i)$ (using the same i). Thereafter, the HA tunnels the packets to both the old and the new CoAddrs of the MN.
- 9) The FA processes the *Registration Reply* and relays the message to the MN.
- 10) After completing the registration process, the MN re-associates with the new AP and deregisters its old CoAddr. The *Deregistration* message is authenticated and validated as the *Registration Request*.

V. EVALUATION

One of the security problems of Mobile IP is vulnerability to DoS attacks due to spoofed registration and deregistration requests. To prevent this attacks, we need to enforce mutual authentication between an MN and its HA.

Mutual authentication between the MN and the MIP entities HA and FA is achieved at the cost of two more key associated to the SDP, stored in the RS. Both HA and the FA will ask the RS to authenticate the MN associated to a particular SDP when a *Request* message arrives.

By using two separate keys, one for *Requests* and another for *Responses*, we ensure that no MIP agent in the network possesses a $MK_{req}(i)$ key required to impersonate a MN.

Concerning the mutual authentication between MIP agents, we considered that this problem is solved by the network provider. For our security requirements all that is needed is a security association between each MIP agent and the RS, to ensure a proper distribution of $MK_{resp}(i)$ keys, identified by an SDP, to MIP agents.

By default, a MN trusts the information provided by a genuine AP; the issue is to distinguish a genuine from a rogue AP. Such separation is already achieved at link layer, because 802.1X provides the MN with key material suitable for authenticating the AP (and vice-versa). Therefore, the MN can authenticate the origin of MIP advertising information (network prefix, FA IP address, etc.) distributed by APs in 802.11 *Authentication Response* messages. Nevertheless, the MN may still be fooled by compromised APs.

VI. RELATED WORK

In [8] it was proposed the Public Key Based Secure Mobile IP (MOIPS), which was built upon a DNS-based X.509 public key infrastructure. This system was developed to implement three basic services concerning security on MIP:

- 1) Authentication of MIP control messages for location updates within CNs.
- 2) Access control of a MN to use resources in foreign networks. A FA can verify the identity of a MN before allowing it to complete its registration and connect to the

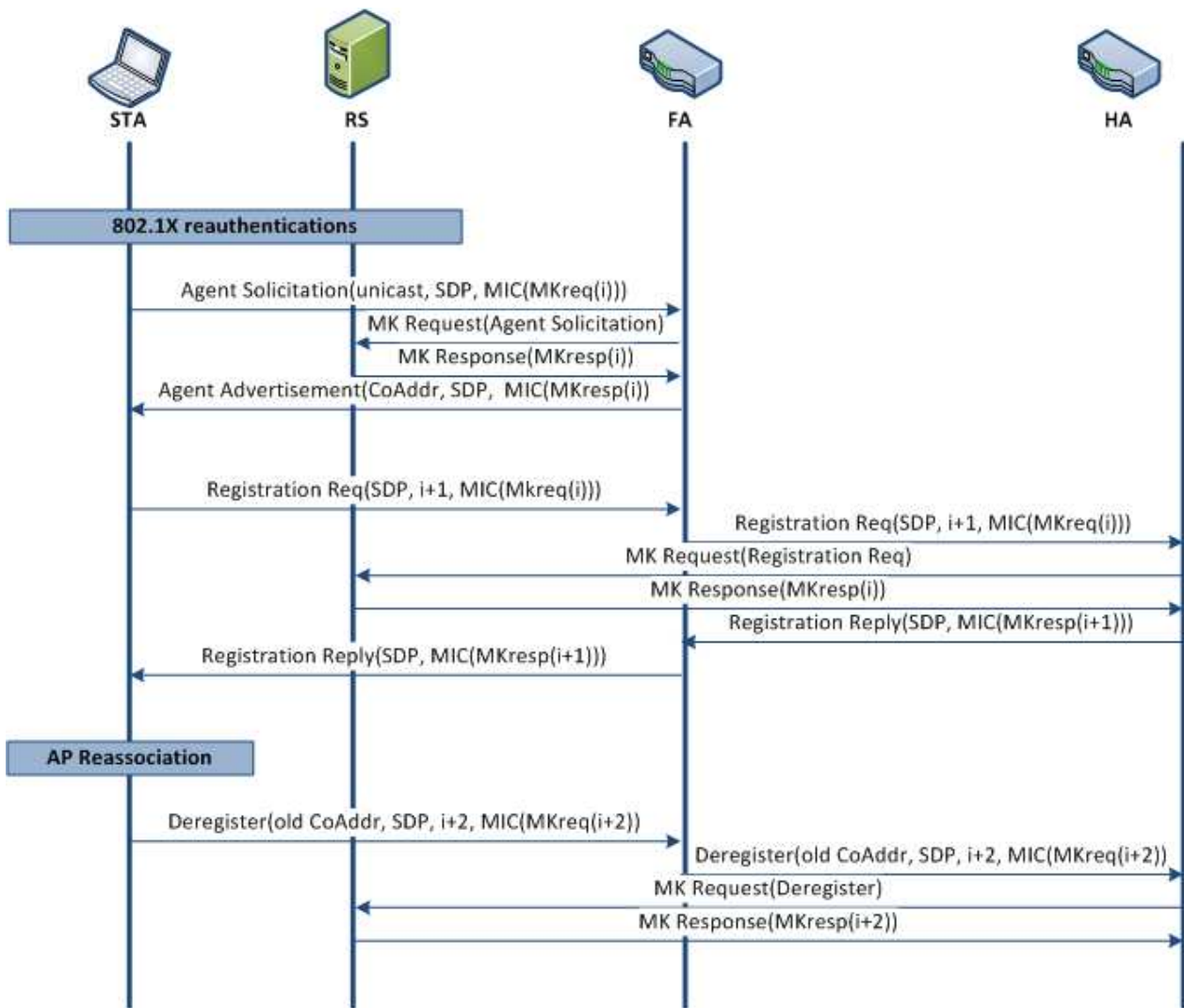


Fig. 3. Protocol description of an STA roaming to a subnet with a FA.

new network. The access control procedures are based on the current network affiliation of the MN, which should be derived from its current identity.

- 3) Secure tunnels between mobility agents (HA and FA) to redirect packets. To protect tunnels, IPsec in tunneling mode is deployed.

The MOIPS architecture uses a public key infrastructure (PKI) for managing X.509 v.3 public keys certificates and v.2 certificate revocation lists (CRLs). The identity and network affiliation of both end nodes' addresses (MN and CN) and mobility agents (HA and FA) are bound to public key certificates issued to these network entities. The exchange of these certificates and the demonstration of possession of the corresponding private keys may allow all sorts of bilateral authentication between end hosts and mobility agents. MOIPS relies on the Domain Name System (DNS) as the primary certificate repository.

MOIPS was designed for large scale, intra-domain mobility and for protecting interactions with CNs. But certificate

issuing represents a challenge, namely the management of their lifetime and the related management of CRLs. Certificate validation also represents a challenge, since it requires a world-wide PKI. Finally, binding IP address to public key certificates and using DNS for distributing them simply cannot be used when MNs are bound to private IP addresses, which is quite common.

Our approach was totally different from the one of MOIPS because we only tried to handle intra-domain mobility within (possibly large) organizations. Intra-domain mobility allows different domains to implement different sorts of local mobility protection policies while allowing hosts to roam locally. Therefore, we do not need a world-wide security infrastructure for protecting MIP interactions, as mobility is confined to and controlled within each security domain.

In [3] was presented an authentication mechanism for a MN in foreign networks that promotes fast handovers. They assume an authentication architecture with a Home AAA service (AAA_H) and a Local AAA service (AAA_L), locally

used in the visited networks. These authentication services are used to generate and distribute session keys to MIP entities (MN, FA and HA). The main contribution is a fast authentication mechanism for MNs in several foreign networks served by different FAs. Broadly, the mechanism migrates security contexts among FA to avoid high-latency interactions with AAA services.

Their approach is different from ours in two main aspects. First, the authentication architecture is different, as we assume that there is only one authentication service for the MIP environment, implemented by the RS. Since the RS is used for fast, link layer handovers, we can naturally assume that it is close and fast enough for enabling authentications required by MIP. Second, in our case FAs do not need to handle migration of contexts for fast handover because we are able to register two CoAddr addresses of a MN in its HA during its 802.11 reassociation to minimize the impact of handovers.

VII. CONCLUSION

In this paper, we present a method that performs lower latency handovers in a security domain while using the default MIP protocol by itself with origin authentication. Compared with existing approaches, we do not add complexity to MIP, and we only introduce the RS to the message authentication process. As a result, it is possible to obtain a secure environment for performing handovers protecting all the entities involved without relevant performance penalties. Furthermore, the overall management of the security domain remains fairly simple and based on the 802.1X architecture. The main security setup activities for deploying the proposed MIP security are the required security associations between RS and local MIP mobility agents (local HAs and FAs). Finally, with the proposed security architecture for MIP we integrate the management of both link layer and network layer mobility, which facilitates the administration and coherence of the security domain.

REFERENCES

- [1] R. Droms. Dynamic Host Configuration Protocol. RFC 2131, IETF, March 1997.
- [2] C. Kaufman. Internet Key Exchange (IKEv2) Protocol. RFC 4306, IETF, December 2005.
- [3] Hyun Gon Kim, Doo Ho Choi, and Dae Young Kim. Secure Session Key Exchange for Mobile IP Low Latency Handoffs. In *Int. Conf. on Computational Science and Its Applications (ICCSA 2003)*, pages 18–21, Montreal, Canada, May 2003. Lecture Notes on Computer Science (LNCS 2668).
- [4] Rodolphe MArques and André Zúquete. Fast, Secure 802.11 Handovers: Back to the Basis. In *4th ACM International Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet 2008)*, Vancouver, British Columbia, Canada, October 2008. (to appear).
- [5] M. Nakhjiri and Y. Ohba. Derivation, delivery and management of EAP based keys for handover and re-authentication. IETF HOKEY WG Internet-Draft, November 2007. draft-ietf-hokey-key-mgm-01.
- [6] C. Perkins. IP Mobility Support for IPv4. RFC 3344, IETF, August 2002.
- [7] J. Salowey, L. Dondeti, V. Narayanan, and M. Nakhjiri. Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK). IETF HOKEY WG Internet-Draft, November 2007. draft-ietf-hokey-emsk-hierarchy-02.
- [8] John Zao, Stephen T. Kent, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, and Isidro Castineyra. A public-key based secure mobile ip. *Wireless Networks*, 5(5):373–390, 1999.