

Network-Layer Assisted Mechanism to Optimize Authentication Delay during Handoff in 802.11 Networks

Rafa M. Lopez^a, Ashutosh Dutta^b, Yoshihiro Ohba^a, Henning Schulzrinne^c, Antonio F. Gómez Skarmeta^d

^aToshiba America Research Inc., ^bTelcordia Technologies
Piscataway, New Jersey, USA

^cColumbia University, New York, NY 10027, ^dUniversity of Murcia, Spain

Abstract—Secured and seamless mobility across heterogeneous access networks needs optimization at all layers. Authentication and security association at the link layer is one of the major components of delay during handoff. We propose a network-layer assisted proactive handoff scheme that helps to optimize the handoff process involving link-layer security across multiple subnets. We demonstrate this proactive scheme and analyze the results for IEEE 802.11-based networks for both roaming and non-roaming scenarios. We then compare these results with the pre-authentication techniques offered by IEEE 802.11i.

Keywords - Mobility; Security; Handoff; Optimization

I. INTRODUCTION

Wireless Internet Service Providers (WISPs) envisage supporting real-time applications in WLAN, such as Voice over Internet Protocol (VoIP), as a promising business. However, the service providers need to take into account the effect of terminal mobility during handoff between WLANs. In order to provide desirable quality of service for interactive VoIP and streaming traffic, one needs to limit the value of end-to-end delay, jitter, and packet loss to a certain threshold level. ITU-T and ITU-E standards define the acceptable values for these parameters. For example, for one-way delay, ITU-T G.114 recommends 150 ms as the upper limit for most of the applications, and 400 ms as generally unacceptable delay. One way delay tolerance for video conferencing is in the range of 200 to 300 ms. Thus, handoff between the WLAN networks requires a solution that can provide seamless mobility service and desired quality of service for real-time applications, such as VoIP.

Actually, providing seamless mobility is one of the most important challenges in WLAN, but it becomes more challenging when security is added on the top of mobility and AAA (*Authentication, Authorization and Accounting*) is included as part of the security signaling. Fig. 1 shows a basic Internet roaming scenario where two different administrative domains that are managed by different WISPs establish business agreements between them in order to provide roaming services for their customers. In particular, these business relationships allow users who belong to one domain (*Home Domain*) to access the network and services in other domains (e.g., *Roaming Domain A* or *Roaming Domain B* in the Fig. 1). A domain here is defined as an administrative domain. There

may be several subnets within an administrative domain. These agreements are enforced by means of the deployed AAA infrastructures (e.g., AAAv, AAAh) in each domain. In nutshell, the home AAA domain (where the user belongs to) is equipped with a home AAA (AAAh) and each roaming AAA domain is equipped with an AAA proxy (AAAv) that contacts the home AAA infrastructure in order to verify the roaming user's credentials.

Fig. 1 also highlights three different types of movement: intra-subnet, inter-subnet and inter-AAA-domain (or inter-domain hereafter). Link-layer handoff is the common scenario in this roaming architecture. Thus, certain optimization on the establishment of security during link-layer handoff deserves some attention.

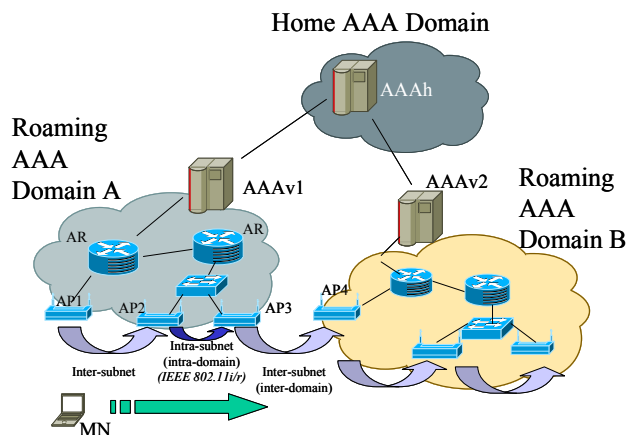


Figure 1: Wireless Internet Roaming Scenario

While the effort is underway to optimize this delay, little has been done to optimize the link-layer security establishment and authentication processes that involve inter-subnet and inter-technology handoff. Particularly for WLAN networks, IEEE 802.11 Working Group and other researchers have been looking into solutions that can provide the desired quality of service and secure seamless mobility between two IEEE 802.11 networks.

Mainly the IEEE 802.11i and 802.11r specifications have contributed to reduce the delay due to link-layer authentication

and security establishment during handoff. In general, these specifications propose a set of mechanisms and handoff signaling to achieve seamless mobility with security. However, these mechanisms are designed to work at link-layer level which entails some implications and limitations for inter-technology and inter-subnet handoff, such as the inability to pre-authenticate. We propose and demonstrate a novel architecture based on pre-authentication at network-level that assists the existing IEEE 802.11 handoff optimization mechanisms involving security by overcoming these limitations and improving the overall handoff delay.

This paper is organized as follows. In Section II, we describe the related work and provide an overview of the existing link layer techniques for supporting secure fast-handoff in IEEE 802.11 networks. Section III describes the proposed architecture, protocols involved and detailed mechanism of how network-layer assists link-layer handoff optimization mechanisms. We describe a testbed and explain the results obtained from the prototype in Section IV. Finally, Section V concludes the paper.

II. RELATED WORK

As mentioned earlier, IEEE 802.11i [1] and IEEE 802.11r [2] provide link-layer handoff optimization mechanisms that attempt to reduce the delay due to link-layer authentication during a node's mobility. IEEE 802.11i was conceived to provide stronger security to IEEE 802.11 WLAN. It relies on IEEE 802.1X [3] for the authentication and access control of IEEE 802.11 stations (STA). As part of 802.1X, a successful authentication allows both STA and AP (Access Point) to generate a Pairwise Master Key (PMK). Typically, the AP relies on a backend *Authentication Server* (AS) such as an AAA server acting as a termination point of an EAP (Extensible Authentication Protocol) authentication method, in order to verify authentication credentials of the peer and deliver the PMK to the AP, as long as the verification is successful. In case of *Pre-Shared Key* (PSK) mode, STA and AP pre-share a 256 bits key that is used as PMK. Therefore, no EAP authentication is needed.

Moreover, a *4-way handshake* protocol uses the PMK for mutually authenticating STA and AP and establishing fresh *Pairwise Transient Keys* (PTKs) to protect link-layer frames. However, IEEE 802.1X authentication can last from several hundred milliseconds to several seconds [4]. Hence, each time a STA moves from one AP to another, this delay and associated packet loss during the handoff affect the real-time application such as VoIP. In order to overcome this problem, IEEE 802.11i introduces a mechanism of pre-authentication depicted in Fig. 2, where the STA starts a new EAP authentication with the target AP where it is likely to hand off, through its current associated AP. After the EAP authentication has completed successfully, the generated PMK is properly stored at the target AP. When STA finally roams to the target AP, both parties engage the 4-way handshake by using the specific PMK. Therefore, EAP authentication is not performed after the handoff.

By decoupling the authentication and network access

control operations from the handoff, IEEE 802.11i pre-authentication reduces the overall handoff delay. However, 802.11i has also some drawbacks and limitations that are worthy to be mentioned:

- Each IEEE 802.11i pre-authentication involves a full EAP authentication. Consequently, it implies a lot of signaling with the authentication server (AS) during each movement.
- The mechanism does not work when the involved APs belong to different distribution systems (DS), where a distribution system is used to interconnect a set of basic service sets and integrated *Local Area Networks* to create an *Extended Service Set* (ESS). For example, inter-subnet and inter-domain pre-authentication is not possible.
- The full association and 4-way handshake are still required to be finished after the movement.

In this sense, IEEE 802.11r [2] overcomes most of these problems by introducing a three level key hierarchy (started either from a *Master Session Key* (MSK) generated during an EAP authentication or a PSK) and a supporting architecture that allows the STA to perform fast transition between the APs within the same so-called *Mobility Domains* (MD) without the need to run EAP authentication during each movement.

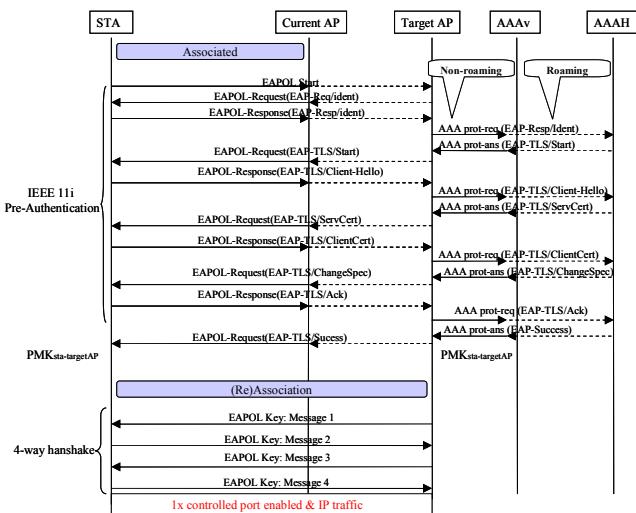


Figure 2: IEEE 802.11i Pre-authentication

Additionally, IEEE 802.11r allows to perform part of the 4-way handshake and some resource reservation at the target AP before STA moves. When STA finally hands off, it only needs to re-associate with the target AP to complete the movement.

Thus, IEEE 802.11r reduces the handoff delay compared to IEEE 802.11i. However, both IEEE 802.11i and IEEE 802.11r mechanisms do not work when the involved APs belong to different distribution systems (DS), which is the case for inter-subnet and inter-domain handoffs. Basically, the reason is that 802.11i and 802.11r handover optimization mechanisms are based on link-layer frames, which cannot operate across different subnets.

The problem of applying link-layer handoff optimization mechanisms between different subnets has also been addressed by the research community. However, most of the solutions are based on *context transfer* mechanisms ([4], [5], [6]). The optimization is achieved by transferring the security context (keys and related parameters) created by STA and previous AP to new AP between subnets. Consequently, STA does not need to run EAP authentication to create a new PMK and only the 4-way handshake is required after the handoff. Thus, the enhancement is achieved in the absence of any link-layer handoff optimization.

For example, Bargh et al [4] explain how to transfer IEEE 802.11i context between two APs under different networks by using a combination of Context Transfer Protocol (CxTP) [7] and Candidate Access Router Discovery (CARD) [8]. Georgiades [5] extends Cellular IP to signal a context transfer between two base stations (BS) under two different gateways (GW). New GW contacts the previous GW to recover security context from previous BS. Duong et al [6] propose an optimized solution also based on CxTP and CARD by proactively transferring a context when MN's move is imminent.

In general, context transfer solutions have some limitations and risks. From the security perspective, it is not always a good idea to transfer the cryptographic keys between different network entities. For example, Housley and Aboba have raised a warning on security context transfer in the Internet Draft [9]. Additionally, to achieve a secure context transfer, one needs to have certain security associations and strong trust relationships between the policy enforcement points such as APs that are not always possible. Finally, it only allows handoff between the same technologies such as 802.11 (*homogenous handoff*).

Mishra et al [10] and Pack et al [11] completely avoid the use of context transfer by pre-installing keys into APs before the STA moves. In general, they are based on algorithms that steer the key installation process based on the movement of mobile node (MN). These solutions assume that an AAA server or trusted third party is in charge of pre-distributing keys to different APs where MN could potentially associate. It implies that AAA server has the knowledge about the location of the APs. This may work when a single WISP is considered. However, in case of roaming scenarios, the home AAA server needs to know the location of the APs in the visited domain. Unfortunately, this is not always possible since, usually, the visited domain shall not want to reveal details about its internal network deployment for privacy purposes, even when roaming agreement has been defined. Additionally, the assumption that an AAA server is able to store the key after EAP authentication is not always true (e.g., RADIUS). Ruckforth et al [12] propose a different approach where a combination of Fast Mobile IPv6 and IEEE 802.11i frames are used to inform user's home domain AAA server about next IPv6 router and next AP where STA may move. With this precise information, AAA server creates a new PMK and sends it to the AP and AR. However, the solution is restricted to IPv6 networks because of the MIPv6 related messages between the access routers. Forte et al, [13] propose a cooperative roaming approach to authenticate the mobile, but its usage is limited to a domain only.

As per the limitation of the existing mechanisms, we have proposed network-layer assisted link-layer pre-authentication mechanism [14], [15]. These mechanisms propose to reduce link-layer handoff latency when existing link-layer handoff optimization mechanisms cannot be applied for cases involving inter-domain and inter-access technologies. The proposed mechanism also preserves the security criterion raised in the IETF [9] by not allowing context transfer between the APs. In this paper, we describe a detailed architecture of this mechanism, provide experimental results from a testbed implementation, describe the benefits our proposal offers, and compare these with IEEE 802.11i pre-authentication.

III. NETWORK-LAYER ASSISTED LINK LAYER PRE-AUTHENTICATION

In this section, we explain the architecture of our proposal. It uses pre-authentication at network-layer to assist link-layer handoff optimization techniques by allowing a fast transition even when the APs involved in the handoff do not share same link layer. Although this mechanism can work independent of link-layer access technologies, we focus our study on 802.11 networks. Authors have introduced the concept of Media Independent Pre-authentication [14] that provides the initial motivation for the bootstrapping of link-layer authentication by means of network-layer authentication. However, we describe and extend this process in more details, and demonstrate the concept with experimental results in a testbed.

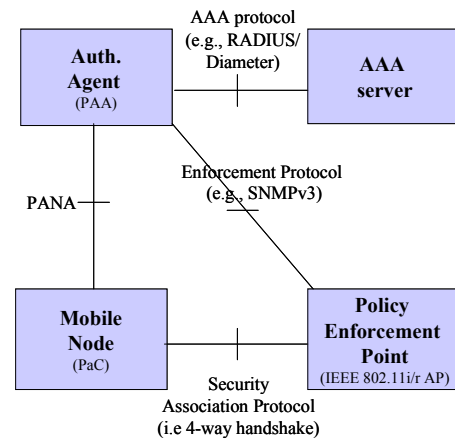


Figure 3: Interaction between Functional Components

Following is a list of some of the features supported by the proposed architecture:

- It works independent of link-layer technology and can thus be applied to IEEE 802.11i, 802.11r or some other technology without changing the characteristics of underlying technology.
- It overcomes the limitations of other link-layer pre-authentication mechanisms such as IEEE 802.11i or 802.11r in inter-subnet and inter-domain handovers.
- It allows a smooth and fast handoff for scenarios where existing link-layer pre-authentication cannot be applied, such as inter-domain handover.

TABLE I. COMPARISON OF POST-AUTHENTICATION AND PRE-AUTHENTICATION

Types of Authentication	IEEE 802.11i post-authentication		IEEE 802.11i pre-authentication		Network-layer -assisted pre-authentication	
	Non Roaming	Roaming	Non Roaming	Roaming	Non Roaming	Roaming
<i>Tauth</i>	61 ms	599 ms	99 ms	638 ms	177 ms	831 ms
<i>Tconf</i>	--	--	--	--	16 ms**	17 ms**
<i>Tassoc+4way</i>	18 ms	17 ms	16 ms	17 ms	15 ms	17 ms
<i>Total</i>	79 ms	616 ms	115 ms	655 ms	208 ms	865 ms
<i>Handover Delay</i>	79 ms	616 ms	16 ms*	17 ms*	15 ms	17 ms

*This time is only applicable within same DS.

**This time includes key installation for two APs in our testbed.

Fig. 4, EAP-TLS [23] is used as EAP method for the authentication. The PAA can rely on a backend AAA server to carry out an EAP authentication method. Then, MN obtains configuration information that allows it to participate in the new network. From MSK generated during the EAP authentication method, PAA can derive a distinct PSK per AP. PAA installs these keys in those APs (*pre-configuration phase*), and provides the MN with the required information (e.g., APs' MAC addresses) to generate the same PSKs.

Then MN moves to the new AP, and after association, runs a 4-way handshake by using the specific PSK_{ap} generated during PANA pre-authentication. At this point, the handoff is complete. Thus, by pre-authenticating and pre-configuring the link, the security association establishment during handoff reduces to 4-way handshake only.

In comparing IEEE 802.11i pre-authentication presented in Fig. 2 with the PANA-based network-layer pre-authentication showed in Fig. 4, one may notice that both schemes reduce the delay invoked by the authentication process during the handover between access points. In particular, the delay is reduced to the time for the 4-way handshake required to establish a security association between the PaC and the Target AP in both cases. Therefore, in terms of handoff delay, both schemes result in comparable values. However, our proposal allows to obtain the same reduction even when the APs belong to different subnets, that may be part of different administrative domains. Thus, it takes care of the limitation imposed by the regular IEEE 802.11i pre-authentication mechanism.

Another interesting advantage in our proposal is that a PAA can control and distribute PSKs to several APs through a single EAP authentication, the one performed during the pre-authentication shown in Fig. 4. This means that, although two messages are required for key installation, when PaC moves between the APs covered by the same PAA's area, we avoid the signaling needed by EAP authentication. As depicted in Fig. 2, EAP authentication typically involves several roundtrips to the backend AAA infrastructure. Thus, our proposed scheme avoids a full EAP authentication in contrast with 802.11i pre-authentication where a full EAP authentication is performed during each handoff.

E. PSK Derivation

During PANA pre-authentication, a *Master Session Key* (MSK) is generated after EAP authentication. The MSK is used to derive a *PaC-EP-Master-Key*, specific for both AP and MN. In turn, the PaC-EP-Master-Key is used to derive the PSK.

Since the PSK is dynamically derived from PaC-EP-Master-Key, it has an associated lifetime. In PANA, the PaC-EP-Master-Key lifetime (and thus the PSK lifetime) is bounded by the PANA security association lifetime which, in turn, is bounded by the MSK lifetime. Since each EAP re-authentication generates a new MSK, new PaC-EP-Master-Key and PSK are derived. For security reasons, when a new PSK is installed in the AP, the 4-way handshake must be run immediately. It allows to generate new fresh PTKs from the new PSK. It is worth mentioning that, in general, PaC-EP-Master-Key can be used for bootstrapping link-layer security at Policy Enforcement Points (PEP) of any link-layer types (e.g., either 802.11 or CDMA), which allows MN to roam among multiple PEPs of different link-layer types without additional EAP execution if the PEPs are controlled by the same PAA.

F. Key Installation Process

We consider two key installation methods, namely, *pre-emptive* (default method in PANA) and *on-demand*. As part of pre-emptive installation process, the PAA installs PSKs in a *pre-emptive* way in all target APs. However, this introduces scalability and resource consumption problems when many APs are under control of one PAA or many MNs are connected to APs served by one PAA. Since it provides the needed PSK for a particular MN and AP *before* MN is attached, it reduces the time to start 4-way handshake.

Alternatively, an AP may inform the PAA when the MN is associated with it. This mechanism is *on-demand* key installation for the AP. Although this mechanism can save resources, it introduces a delay to gain network access because both MN and AP need to wait for the PSK provisioning. Moreover, if some kind of AP association notification is used as a trigger of PSK installation, the key installation process is triggered by an event generated from unauthenticated information.

In order to take advantage of both methods and minimize some of their disadvantages, algorithms such as those proposed in [10] and [11] could be used. These algorithms determine the most probable APs where MN may move to, so that PAA can install PSKs only at those APs selected by the algorithm, as part of pre-emptive key installation. However, if the prediction fails and MN finally moves to another AP where PSK has not been installed, on-demand key installation may be used instead. Depending on the number of APs and the number of users, a WISP may decide to use one or another technique or even a combination of both.

G. Key Installation Synchronization

As we may observe in Fig. 4, in the typical key installation phase, the process is started by the PAA just after receiving the *PANA-Binding-Answer* (PBA). Additionally, the key installation may last a non-negligible time. Therefore, in certain cases, when the MN decides to move immediately after sending the PBR or, even, the PBR is lost, the key installation process may not have finished. This may result in mobile not getting connected to the new AP without any PSK.

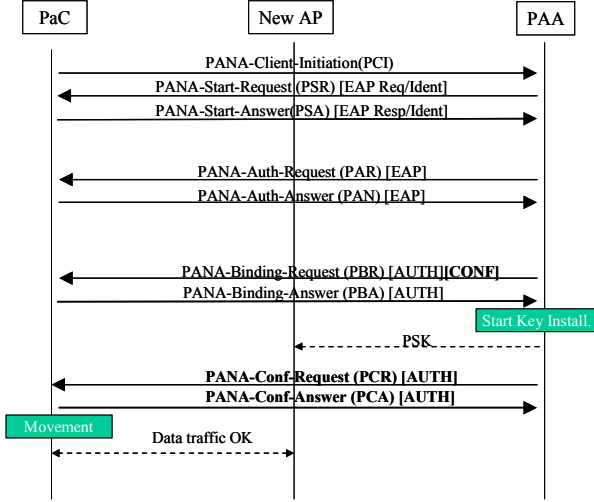


Figure 5: New PANA Messages for Configuration

In order to avoid this race condition, we have expanded the PANA design as shown in Fig. 5 in order to support a pair of (optional) new messages (*PANA-Conf-Request* and *PANA-Conf-Answer*) used to signal the PaC that the key installation process has been successfully finished. Additionally, we have added a new flag *CONF* in the PBR message in order to inform the PaC that it should wait for the PCR message before the handover. For simplicity, in the testbed, we assume that the pre-configuration process (key installation) completes before the handover starts.

IV. TESTBED PROTOTYPE AND RESULTS

We have implemented the proposed mechanism in a testbed as shown in Fig. 6. We illustrate different scenarios and demonstrate how network-layer pre-authentication can provide link-layer handoff optimization mechanism. In particular, we apply the pre-authentication mechanism over IEEE 802.11i and compare the results with the existing pre-authentication mechanism for IEEE 802.11i.

A. Testbed Details

We have used hostapd software [24] and madwifi driver [25] and have configured three Linux systems to act as access points. Two of them (AP1 and AP2) work as IEEE 802.11i APs. Both of these APs may work in either PSK (when network-layer pre-authentication is used) or 1X EAP mode. This also provides inbuilt RADIUS client functionality within the AP (for the cases where network-layer pre-authentication is not enabled). Each AP implements a SNMPv3 agent that

allows it to set PSKs and associated parameters such as key lifetimes. Finally, the last access point (AP0) is configured with open authentication. The MN is a laptop equipped with wpa_supplicant software [24] that provides 802.11i functionality, madwifi driver, and Open Diameter’s PANA client implementation [26]. PANA agent is based on Open Diameter implementation that also provides inbuilt Diameter Client [26]. We have used Open Diameter [26] and Free Radius [27] as the AAA protocol implementations.

Fig. 2 illustrates the protocol interaction when IEEE 802.11i pre-authentication is used. Moreover, Fig. 4 shows the protocol interaction between different network components that demonstrate network-layer assisted pre-authentication. All our experimental scenarios use EAP-TLS [23] as EAP method to authenticate the MN.

B. Experimental Scenarios

We have experimented with three types of movement scenarios involving both roaming and non-roaming cases. In the *roaming case*, MN is visiting in an administrative domain that is different than its home domain. Consequently, the AAAh, which is placed in a different continent in our experiment, needs to be contacted. For the *non-roaming case*, we assume the MN is moving within its home domain and only local AAA server (AAAv) is contacted.

The first scenario does not involve any pre-authentication. The MN is initially connected to AP0 and moves to AP1. Because neither network-layer authentication is enabled nor IEEE 802.11i pre-authentication is used, MN needs to engage in a full EAP authentication with AP1 to gain access to the network after the move (*post-authentication*). This experiment shows the effect of delay when there is no pre-authentication.

The second scenario involves 802.11i pre-authentication and involves movement between AP1 and AP2. MN is initially connected to AP2, and starts IEEE 802.11i pre-authentication with AP1. This is an ideal scenario to compare the values obtained from 802.11i pre-authentication with that of network-layer assisted pre-authentication. Both the first and this second scenarios use RADIUS as AAA protocol with the APs implementing a RADIUS client.

The third scenario takes advantage of network layer assisted link-layer pre-authentication. It involves movement between two APs (e.g., between AP0 and AP1) that belong to two different subnets where 802.11i pre-authentication is not possible. Here, Diameter is used as AAA protocol where PAA implements a Diameter client.

In this third movement scenario, MN is initially connected to AP0. MN starts PANA pre-authentication with the PAA which is co-located on the AR in the new candidate target network (nAR in network A) from the current associated network (network B). After authentication, PAA installs two keys, PSK_{ap1} and PSK_{ap2} in both AP1 and AP2 respectively by using a pre-emptive key installation method. Finally because PSK_{ap1} is already installed, AP1 starts immediately the 4-way handshake upon mobile’s arrival.

As observed, we have used the same target access point AP1 to perform the handover for all the three scenarios.

Therefore the 4-way handshake time measurement is always taken at this access point. For the first scenario, the mobile node (MN) is initially attached to AP0 because we try to simulate the case when 802.11i pre-authentication cannot be executed. This happens when the target AP (AP1) is not placed in the same DS as current AP (AP0). For the second scenario, both AP1 and AP2 are configured with 802.11i support, so that one can simulate 802.11i-based network protection. Therefore, in order to initiate a handoff to AP1, the MN starts the test attached to AP2 after running an initial EAP authentication. Finally, for the third scenario, the MN is initially attached to AP0 and the handoff is performed to AP1. In this case, we simulate the scenario where 802.11i pre-authentication cannot be performed and network-layer can be used instead.

We have used the ethereal and kismet measurement tools to analyze the measurements for the 4-way handshake and PANA authentication. These measurements reflect different operations involved during network-layer pre-authentication.

C. Analysis of the Results

Scanning, authentication and association are part of the link-layer handoff delay. From our experiments we have obtained a mean value of ~460 ms as the scanning time in our testbed environment. Shin et al [28], [29] provide some interesting results in reducing the scanning time. Additionally, by retrieving information about the neighboring APs before handoff, it helps the MN to communicate with the network elements in the target networks before the MN moves. Prior discovery of the details of APs can reduce the number of APs to be scanned during handoff and can even completely avoid it. In particular, MN may rely on outside mechanisms such as 802.21 [21] to discover neighboring APs as we have mentioned in Section III.C.

In our experiment, as part of the discovery phase, we assume that the MN is able to retrieve PAA's IP address and all required information about AP1 and AP2 (e.g., channel, security-related parameters, MAC address) at some point before the handover. This avoids scanning during link-layer handoff. We have applied this assumption to all three scenarios. Because our focus is on reducing the time spent on authentication part during handoff, we do not discuss the details of how we avoid the scanning. Details of this mechanism could be found in [30].

Table 1 shows the timing (rounded off to the most significant number) associated with some of the handoff operations we have measured in the testbed. We describe each of the timing below.

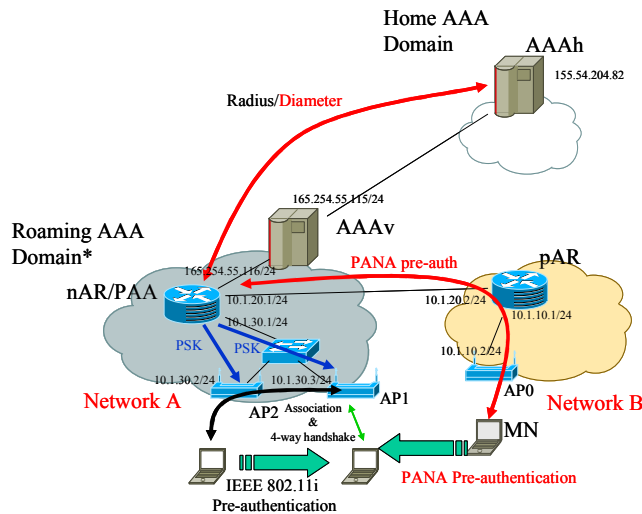
- T_{auth} refers to the execution of EAP-TLS authentication. This time does not distinguish whether this authentication was performed during pre-authentication or a typical post-authentication.
- T_{conf} refers to time spent during PSK generation and installation after EAP authentication is complete. When network-layer pre-authentication is not used, this time is not considered.

- $T_{assoc+4way}$ refers to the time dedicated to the completion of association and the 4-way handshake with the target AP after the handoff.

We show the total time in the process by adding these quantities. Finally, we also highlight the time that affects the handoff in each case.

Each of these timings may safely be considered as independent per each experiment. Thus, the authentication phase, the configuration phase, and the association or 4-way handshake can be considered as independent events. In fact, $T_{assoc+4way}$ time seems to be similar in value regardless of the movement scenario. Also, independent of whether PANA was run on roaming or non-roaming case, value of T_{conf} remains same.

The first two columns in Table 1 show the results for non-roaming and roaming cases, respectively, when no pre-authentication is used. The second two columns depict the same cases when IEEE 802.11i pre-authentication is used. Finally, the last two columns show when we used network-layer pre-authentication. When pre-authentication is used, only the $T_{assoc+4way}$ affects the handoff time. When no pre-authentication is used, the time affecting the handoff includes T_{auth} (the complete EAP-TLS authentication) plus $T_{assoc+4way}$.



* Roaming AAA Domain in roaming case.
For non-roaming case, it acts as MN's home AAA domain.

Figure 6: Testbed Architecture

That is equivalent to the time affecting the handoff in the case where MN moves from AP0 to AP1 in the absence of pre-authentication. As it is seen, these delays are not suitable for real time applications. Indeed, for non-roaming case, we obtained a ~80 ms delay for re-establishing the connection with target AP1. It takes about 600 ms to complete the handoff when MN moves to a visited domain and home AAA server is placed far. However, network-layer pre-authentication is only affected by $T_{assoc+4way}$ (~17 ms) during any kind of handoff authentication. As evident, IEEE 802.11i pre-authentication provides a comparable benefit (~16ms) in terms of handoff but

is limited to cases when APs are in the same distributed system (DS). The difference in values could be contributed to margin of error during experiments. Additionally, network-layer pre-authentication leverages a single EAP authentication to bootstrap security in several target APs, by allowing MN to move among APs under same PAA without running EAP and, consequently, without contacting the AAA server. In this sense, it extends the advantages offered by IEEE 802.11r over IEEE 802.11i technology by allowing inter-subnet, inter-domain, and inter-technology handoffs.

Finally, it should be noted that, during PANA-based pre-authentication, times T_{auth} and T_{conf} spent for the EAP authentication and the key installation, respectively, depend upon PAA's location with respect to the AP. In normal circumstances, if the PAA is placed farther from APs, these times will increase correspondingly. However, in our architecture, placement of PAA does not affect the handover delay since many of these operations are done ahead of time. Pre-authentication time will be a significant factor for a highly mobile user that is subjected to consecutive handoff. It is essential that the pre-authentication be done ahead of time so that it completes before the next link-layer handoff starts.

V. CONCLUSIONS

Security related handoff optimization at link-layer can contribute to fast secure and seamless mobility for the roaming users. Proposed network-layer assisted mechanism and results of the prototype demonstrate that it can provide comparable performance at link-layer similar to the existing mechanisms such as pre-authentication for IEEE 802.11i.

Additionally, the proposed mechanism can eliminate the limitation of the existing link-layer security optimization and can be used for both roaming and non-roaming scenarios involving inter-subnet, inter-technology and inter-domain handoff where the existing link-layer security optimization is not sufficient. Although our results have focused on 802.11 only, this mechanism can very well be extended to support handoff between inter-access technologies such as 802.11, 802.16, and CDMA. As part of the future work, we will consider other deployment scenarios including heterogeneous access technologies, and plan to experiment with media independent pre-authentication techniques that can optimize the handover process between different access technologies.

ACKNOWLEDGMENT

Authors would like to acknowledge Kenichi Taniuchi and Victor Fajardo of ITSUMO project for their help during prototype development. R. Marin Lopez would specially like to thank to Julien Bournelle for PANA and IEEE 802.11i related discussions. Antonio F. Gomez would like to acknowledge people involved in the ENABLE (Enabling Efficient and Operational Mobility and Large Heterogeneous IP Networks, IST2005-027002) EU IST project and DAIDALOS (Designing Advanced network Interfaces for the Delivery and Administration of Location independent, Optimized personal Services, FP6-IST026943) EU IST project.

REFERENCES

- [1] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security", IEEE std. 802.11i, July 2004
- [2] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 8: Fast BSS Transition", IEEE std. 802.11r
- [3] Institute of Electrical and Electronics Engineer, "IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control", IEEE std. 802.1X-2004.
- [4] M.S Bargh et al, "Fast Authentication Methods for Handovers between IEEE 802.11 Wireless LANs", ACM WMASH'04, October 2004, Philadelphia
- [5] M. Georgiades, "Context transfer support for IP-based mobility management", CCSR Awards for Research Excellence 2004
- [6] H. Duong, A. Dadej and S. Gordon, "Proactive Context Transfer in WLAN-based access networks, Proceedings of 2nd ACM International Workshop on Wireless Mobile Applications and Services, Oct. 2004, Philadelphia
- [7] J. Loughney, M. Nakhjiri, C. Perkins and R. Koodli, "Context Transfer Protocol (CXTTP)", RFC 4067, July 2005.
- [8] M. Liebsch, A. Singh (Ed.), "Candidate Access Router Discovery," IETF RFC 4066, July 2005.
- [9] R. Housley and B. Aboba, "Guidance for AAA Key Management", draft-housley-aaa-key-mgmt-09.txt, IETF, Work in Progress, Feb 2007
- [10] A. Mishra, M. Shin, N. Petroni, C. Clancy and W. Arbaugh, "Proactive Key Distribution Using Neighbor Graphs", IEEE Wireless Communication, February 2004
- [11] S. Pack and Y. Choi, "Fast Inter-AP Handoff using Predictive-Authentication Scheme in a Public Wireless LAN", IEEE Networks 2002
- [12] T. Rückforth, Y. Roudier and J. Linder "AAA Context Transfer for Fast Authenticated Inter-Domain Handover", Technical Report, September 2004
- [13] A. Forte and H.Schulzrinne, "Cooperation Between Stations in Wireless Networks, Columbia University Computer Science Technical Report
- [14] A. Dutta , Y. Ohba, V. Fajardo, K. Taniuchi and H. Schulzrinne, "A Framework of Media-Independent Pre-Authentication", draft-ohba-mobopts-mpa-framework-05, IETF Work in Progress, Mar 2007
- [15] R. Marin-Lopez, Y.Ohba and Julien Bournelle, "PANA bootstrapping IEEE 802.11 security", draft-marin-pana-ieee80211doti-00.txt, March 2006, IETF Work in Progress
- [16] D. Forsberg, Y. Ohba, B.Patil, Hannes Tschofening and A.Yegin, "Protocol for Carrying Authentication for Network Access", IETF Draft, March 2007, IETF Work in Progress
- [17] C. Kauffman (Ed.), "Internet Key Exchange (IKEv2) Protocol", IETF, RFC 4306, December 2005
- [18] Y. Ohba, "Pre-authentication Support for PANA", draft-ietf-pana-preauth-01, IETF Draft, March 2006, IETF Work in progress
- [19] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.
- [20] P. Calhoun, J. Loughney, E. Guttman, G. Zorn and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003
- [21] IEEE P802.21/D05.00, Draft IEEE standard for Local and Metropolitan Area Networks: Media Independent Handover Services, April 2007
- [22] A. Dutta et al. "Seamless Handoff across Heterogeneous Networks - An 802.21 Centric Approach", IEEE WPMC 2005, Aalborg, Denmark
- [23] B. Aboba and D. Simon, "PPP EAP TLS Authentication Protocol ", RFC 2716, October 1999
- [24] Host AP software, <http://hostap.epitest.fi/>
- [25] MADWiFi Driver, <http://sourceforge.net/projects/madwifi/>
- [26] Open Diameter, <http://sourceforge.net/projects/diameter/>
- [27] Free Radius, <http://www.freeradius.org/>
- [28] M. Shin, A. Mishra and W. Arbaugh, "Improving the Latency of 802.11 Hand-offs using Neighbor Graphs", ACM MobiSys 2004, Boston, MA
- [29] S. Shin, A. Forte, A. Rawat, H. Schulzrinne, "Reducing MAC Layer Handoff Latency in IEEE 802.11 Wireless LANs," Proceedings of ACM MobiWAC, September 2004
- [30] A. Dutta et al, "MPA-assisted Proactive Handoff Scheme," ACM Mobiquitous, 2005, San Diego, CA