Measurement and Analysis of Handover Latencies in IEEE 802.11i Secured Networks

Ivan Martinovic, Frank A. Zdarsky, Adam Bachorek, and Jens B. Schmitt
disco | Distributed Computer Systems Lab, University of Kaiserslautern, Germany
{martinovic,zdarsky,a_bacho,jschmitt}@informatik.uni-kl.de

***Abstract*— The purpose of the IEEE 802.11i standard is to endue wireless networks with advanced security by leveraging mature and proven security technologies. The concept of a *Robust Secure Network* (RSN) as a long-term security architecture was defined in order to provide confidentiality of data being transferred over the wireless medium as well as to provide mutual authentication between mobile stations and the network infrastructure. Nonetheless, security provisioning is indubitable time and resource consuming, which poses a problem as far as meeting quality of service demands of forthcoming delay-critical applications (e.g. Voice over WLAN) is concerned.**

The main objective of this research is to measure and analyze how currently deployed mobile devices perform when joining the RSN as defined by the IEEE 802.11i security amendment. Furthermore, we investigate various state-of-the-art implementations of IEEE 802.11i among different mobile devices providing the answer to what to expect on performance sacrifice by utilizing link-layer protection of IEEE 802.11i.

As a result of this work, we find that the price to pay for the IEEE 802.11 security greatly varies among different devices, starting from low latencies such as ≈19 ms up to ≈330 ms and interestingly, computational stronger clients are not a priori the winners.

***Index Terms*— WLAN, Security, IEEE 802.11i, Measurement.**

I. Introduction

Ever since IEEE 802.11 [1] became the first widely-approved wireless data networking standard, Wireless Local Area Networks (WLANs) have exhibited significant growth regarding corporate as well as home networking environments. Yet, a weak encryption algorithm, no proper integrity check and a replayable authentication method amongst others were the causes for the failure of the legacy security features known collectively as Wired Equivalent Privacy (WEP) to ensure the fundamental security objectives.

The anticipated solution to the existing security inadequacies was finally presented in mid 2004 when IEEE successfully ratified its 802.11i [2] security standard, the first products for PDAs appeared in late 2005. The cornerstone of this standard is the concept of separating the user authentication and the message protection process which allows for embedding many currently stationary-approved authentication protocols like Kerberos and Extensible Authentication Protocol (EAP) with Transport Layer Security (TLS) [5] into the wireless networking domain. Another extension with regard to data confidentiality and integrity is the introduction of a not yet outperformed cryptographic algorithm named Counter Mode with Cipher-block chaining with MAC Protocol (CCMP). Based upon the Advanced Encryption Standard (AES) CCMP provides for strong data encryption and reliable data origin authenticity. Taking the full set of security requirements of the complete ratified IEEE 802.11i [2] into account, the Wi-Fi Alliance released the WPA2 certification programme in the end of 2004 in order to carry on accounting for product interoperability of any vendor.

It is evident that such substantial enhancements involve additional processing complexity and communication between participating network entities which in turn results in corresponding time consumption. Furthermore, to fully utilize IEEE 802.11i the existing infrastucture requires an extension to allow mutual authentication (i.e. using RADUS server) and more computational advanced hardware for implementation of CCMP algorithm. As a result, most of the Wireless Internet Service Providers (WISPs) have abandon link-layer security by using proprietery solutions based on Web-based authentication. This trading of link-layer security has a high impact on overall users' security and imposes new vulnerabilities as shown in [8].

The main contribution of this work is to analyse to what extent the IEEE 802.11i affects the entire handover process of wireless stations. Furthermore, we are interested in the state-of-the art implementations and effects of amendatory standard features like pre-authentication and key caching, and to what extend they provide relief on latencies within a mobile scenarios.

The remainder of this paper is organized as follows. Subsection I-A provides the related work of this subject. The brief introduction of IEEE 802.11i is presented in II. Main part of this research consisting of Section III and its subsections examines common 802.11i wireless network in a mobile scenario. Section V concludes the paper summarizing the results of the measurement campaign.

A. Related Work

One of the most sought-after and at the same time most challenging task within IEEE 802.11 networks is the reduction of connection time delay which still poses a grave problem to real-time applications insisting on upper latency bounds. Attending to this issue, empirical studies in [14], [11], [13] substantiate that more than 90 % of the overall handover delay is to be attributed to the network discovery procedure, which means the detection of absent connectivity leading to the need of a handover in the first place and the corresponding scanning

for available wireless networks. Particularly in [14] and [11], sundry network components, i.e. access points and network interface cards of diverse vendors underwent closer scrutiny which helped to verify a significant product diversity with regard to the analyzed metric of handover delay. Whereas most papers discount the detection time in question, experimental trials in [14] reveal it to be the overhead par excellence and trace it back to vendor-specific implementations, which still determine the behavior of network equipment to be distinct despite compliance with supported standards. Most implementations make a STA react on given number of failed transmissions of active scanning on dedicated wireless channels. Rarely, a STA reacts on decreasing connectivity indicated by periodically measured adversarial Signal-To-Noise Ratios (SNRs). In order to enhance this common course of action [14] proposes to either initiate the channel scanning already on two failed retransmissions or alternatively to reduce the common beacon frame interval from 100 ms to 60 ms which reduces the reaction time of a STA suitably without overtaxing the network capacity. Although the standardized active scanning appears to be the most commonly implemented scanning method, the analysis in [11] shows that its effectiveness still depends on vendor specific settings of the minimal and maximal channel waiting time parameters. Adjasting their values adequately is claimed to be optimal in most cases in view of scanning delay reduction. But, as this criterion normally depends on current network load, the ascertained values shell not be deemed to be universally optimal.

While the latter approaches consider the more frequently used active scanning, in [13] the more lightweight method of passive scanning is focused on. Within the scope of the introduced SyncScan a STA tries to get to know the local AP topology anonomously by making use of the time synchronization feature of the Network Time Protocol (NTP) [10].

In [12] the concept of the Neighbor Graph (NG), a data structure which represents the current network topology. Distributing the STAs' context information among all adjacent APs in advance allowed for a significant reduction of the (re-) association delay from about 15.37 ms to 1.69 ms. The concept of Proactive Key Distribution (PKD) is covered by [6]. By the means of a NG, the session key derived by both the STA and the AP is distributed among the adjacent APs and used whenever the STA is up to switch the network access points. The result analysis shows that the delay implied by auxiliary security message exchange can be reduced to 50 ms or rather 70 ms as stated in [7].

Nevertheless, none of these works analysed an overall mobile scenario based on IEEE 802.11i-enabled networks. While some reasons for this lie in the late availability of fully IEEE 802.11i-enabled devices (first versions of IEEE 802.11i implementation for PDAs were available in 2005/2006), most of the related work was focused on improving network discovery, scanning, and key distribution. Although delays resulting from these phases are currently the major handicap in the way to a seamless handover, the IEEE Task Group "r" has been established to provide the standard for the fast BSS handover to support delay critical applications such as VoIP. This Task Group is still working on the new standard, so it is to expect that the delays resulting from network discovery and reassociations are still being subject to optimization. Due to the fact that the IEEE 802.11i has already been ratified, the security-related delays are now considered to be a part of everyday's mobile scenario and their optimization is subject to the implementation.

II. IEEE 802.11I IN A NUTSHELL

The major objective of the IEEE 802.11i specification is the concept of a Robust Secure Network (RSN). This concept is based upon a security framework composed of several known and well approved protocols and techniques to ensure a robust protection of wireless communication within so-called RSN Associations (RSNAs). As logical link layer connections between RSN-enabled network entities, RSNAs offer port-based access control through IEEE 802.1X [3] which defines the basic model for the support of authentication services such as enhanced mutual authentication and key management via EAP. The entities taking part in 802.11i RSNs are stations (STA) which take the role of a supplicant, access points (AP) as authenticators, and authentication servers (AS) which are commonly RADIUS servers [4]. In the following subsections we briefly describe some of the most important security mechanisms provided by IEEE 802.11i. For a more detailed description, we refer the reader to [9].

A. Mutual Authentication

In general, an authentication can be based on passwords, smart cards, certificates or other credentials verifying the proper identity of the communicating entities. However, each EAP method avails itself of different means by which the authentication objectives are supposed to be accomplished, which in turn affects the stage of security it provides and the potential application area it addresses. EAP on its part abstracts from the encapsulated authentication method and enables the AP to forward authentication messages between the STA and AS in the back-end of the network.

As the 802.11i standard does not commit to specify which particular authentication method to employ when implementing an RSN, it is up to the organization or users to decide which one fits best into their existing or target network environment. For this reason and because the introduction of all existing EAP methods would definitely go beyond the scope of this paper, the remainder of this work shall rather focus on the most commonly used and universally approved authentication method known as Transport Layer Security (TLS).

B. Key Management

In RSN environments all keys have a limited lifetime and are organized in a key hierarchy (see Figure 1).

Central to this hierarchy is a 256-bit cryptographic key called the Pairwise Master Key (PMK) which is obtainable in two ways. Either it is derived from a static Pre-Shared Key (PSK) which has to be manually installed on each device prior to communication, or the PMK may be derived from the result

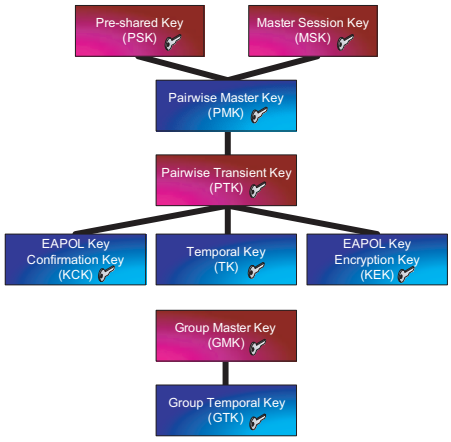

Fig. 1. RSN Key Hierarchy

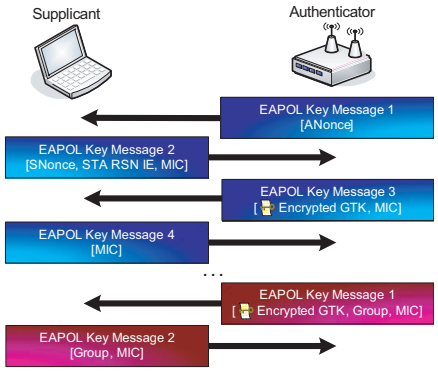

Fig. 2. 4-Way and optional Group Key Handshake message flow

of any method applied in the mutual authentication phase, e.g. the shared session key (henceforth the Master Session Key (MSK)) as the output of the EAP-TLS authentication process. By means of a pseudo random function the PMK is then used to generate the Pairwise Transient Key (PTK), a temporal key for unicast traffic protection from which further encryption and integrity keys like the EAPOL-Key Confirmation Key (KCK), the EAPOL-Key Encryption Key (KEK) as well as the Temporal Key (TK) are extracted. In addition to these unicast keys, in a RSN there may also exist two group keys, the Group Master Key (GMK) and the Group Temporal Key (GTK) as a derivation of the GMK using another pseudo random function. The GTK is defined as the means by which broadcast and multicast traffic protection is made possible.

As for key management in RSNs the IEEE 802.11i security amendment specifies a key generation and distribution scheme. Following a successful EAP-authentication this scheme is meant to perform appropriate operations to generate and derive cryptographic keys and to get them installed into the corresponding devices. The key management phase includes two types of handshakes, a 4-Way Handshake and optionally a Group Key Handshake (see Figure 2).

As the very first step after the mutual authentication process the 4-Way Handshake is initialized by the authenticator to confirm that both authentic entities possess a current PMK, to confirm the cipher suite selection, to derive a fresh PTK from the PMK and to install the encryption and integrity keys as well as the GTK into the corresponding entities. In order to carry out the corresponding message exchange for that purpose EAPOL RSN Key Message frames are used.

During a 4-Way Handshake, four of those frames are exchanged between the STA and the AP. It is initiated by a first completely unprotected message including a random number (ANonce) and being sent by the AP. After generating its own SNonce and extracting the ANonce from the received AP message, the STA is now able to use them along with additional parameters to derive the PTK and all temporal keys from the PMK. This allows for protecting the subsequent message with a Message Integrity Code (MIC) computed using the KCK. When the AP receives this integrity protected message containing the SNonce along with the STA's RSN Information Element (RSN IE) which confirms the cipher suite selection, it can not only derive the PTK and all temporal keys on its part but also is able to verify that the STA is in possession of the current PMK and derived the temporal keys properly. Within the subsequent message the AP includes a KCK-computed MIC and a GTK encrypted with the KEK. The receipt of this frame again lets the STA verify that the AP holds the PMK. The transmission of the fourth and last frame allows the STA to announce that the derived TK will be installed. At this point in time, both entities have proved their knowledge of the previously negotiated PMK to each other and derived the temporal key material needed to protect subsequent data exchange. Thus, after the successful completion of the 4-Way Handshake both entities are mutually authenticated and the STA is qualified to be granted access to the network resources via the controlled service port of the AP.

By contrast, the rarely used Group Key Handshake generally plays a secondary role and conduces to the support of multicast or broadcast application traffic. By means of a two-way exchange of integrity protected EAPOL-Key messages the AP and the concerned STAs may negotiate a new GTK in security jeopardizing conditions in order to preserve their ability to receive protected broadcast or multicast messages. More precisely, the AP simply derives a new GTK, encrypts it with the temporal KEK and passes it to any affected STA which in turn acknowledges the receipt by a subsequent EAPOL-Key message.

C. Pre-Authentication and PMK Caching

In addition to the desired security features previously mentioned, the IEEE 802.11i security amendment introduces two more mechanisms in order to better cope with station mobility and to increase network performance. These mechanisms are Pre-Authentication and PMK Caching also known as PMK Security Association (PMKSA) Caching.

PMKSA Caching conduces to the ability of nearly seamless resumption of previously established secure communication sessions. Therefore, a supplicant and the corresponding authenticator have to store the shared secret which is the afore negotiated or derived PMK. A reason for session resuming

might be the lost wireless connection of a station to its associated AP due to, for instance, radio interference. Reconnecting to the network, a supplicant may prove its eligibility to rejoin the security association by supplying the appropriate ID out of a list of available PMKIDs to the authenticator. Hereupon the caching-enabled authenticator may verify or falsify the ongoing security association depending on whether he finds a match in his PMKID list or not. In the former case, the fact of having cached the negotiated shared secret prevents a station from repeating the entire authentication process and allows for fast re-association with the corresponding AP by merely renewing the PTK out of the PMK via another 4-Way Handshake. But if the handshake fails or the authenticator fails to verify the PMKID, a repetition of the full 802.1X and EAP authentication process becomes inevitable for the access demanding station.

Harnessing the feature of Pre-Authentication, a wireless station is enabled to roam more seamlessly between adjacent APs of an extended service set provided that PMKSA Caching is supported. If so, a station may initiate an authentication process with an authenticator in advance using an existing security association with another AP. Through caching of the established SAs along with the corresponding PTKs this station may then roam between the authenticated APs whenever is needs to, again without having to repeat the entire authentication process. Besides the default network discovery operation, the obligatory final step in authentication for the station to pass through remains the 4-Way Handshake.

After a brief summary of these two performance features, it can be stated that having them enabled within a RSN doubtlessly contributes to a lower network connection delay due to a decimation of the message exchange. Nevertheless, it is to clarify to what extent this factor really improves the matter of intra-subnet handovers and in how far these amendatory mechanisms are already included in currently available implementations.

III. Experimental Scenario

The goal of this work is to provide a detailed insight into latencies encountered within an intra-subnet handover. This includes not only the impact of security mechanisms but also the analysis of the entire network connection process. In our investigation we are interested into the state of the art of the IEEE 802.11i technology realized with off-the-shelf hardware within a typical enterprise network infrastructure as shown in Figure 3.

Furthermore, as the IEEE 802.11i standard leaves enough space for different implementations, we followed every anomaly we experienced trying to find and analyse its cause.

A. RSN Connection Process Overview

Dividing the entire network connection process into its individual steps and discarding the actual secured data transfer phase, five main connection related phases can be identified as shown by Figure 4.

The first phase corresponds to the active or passive network discovery procedure (hence Scanning Phase) of a mobile

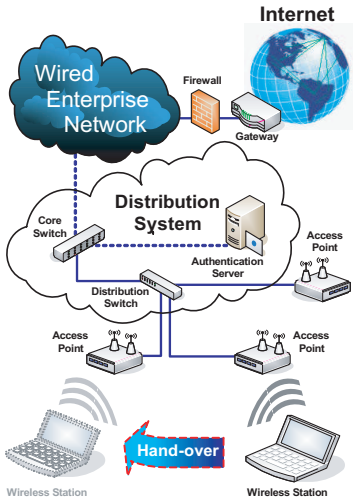

Fig. 3. Layer 2 Handover

station seeking to find appropriate network access points. Both AP messages are expected to comprise the so called RSN Information Element (RSN IE), which announces the APs' RSN capabilities with regard to cipher and key management suite as well as pre-authentication support, subject to the standard. As active scanning was the preferred scanning method applied by all examined STAs, the Scanning Phase in this context is delimited by the first captured Probe Request addressed to the dedicated AP and the Authentication Request initiating the subsequent phase.

The second phase includes the 802.11 legacy authentication and association part which merely serves for backward compatibility and, fundamentally, allows a STA to connect to the uncontrolled port of the AP. This phase begins with the Authentication Request frame sent by the STA and ends with the acknowledgment frame confirming the (Re-) Association Response of the AP.

As already mentioned, this paper focuses on the EAP-TLS combination as a highly secure and well understood authentication method. Therefore, the third phase incorporates the complete EAP-TLS message exchange between the STA and the AS processed via the AP. More precisely, its duration is bounded by the acknowledgement of the (Re-) Association Response frame and the acknowledgement frame confirming the EAP success message which indicates the successful completion of the Mutual Authentication Phase.

At last, the Key Management Phase which executes a 4-Way Handshake, verifies PMK and installs fresh PTK on both supplicant and authenticator concludes the RSNSA establishment process. The 4-Way Handshake is encapsulated within four EAPOL Key messages. Its duration corresponds to the message commutation period from the EAP success acknowledging frame up to the acknowledgement confirming the receipt of the fourth EAPOL RSN Key Message by the STA. Hereupon the protected Data Transfer Phase begins allowing secure and authenticated message delivery and receipt.

Another phase which is worthwhile a deeper study, especially as till now there is no network-triggered handover

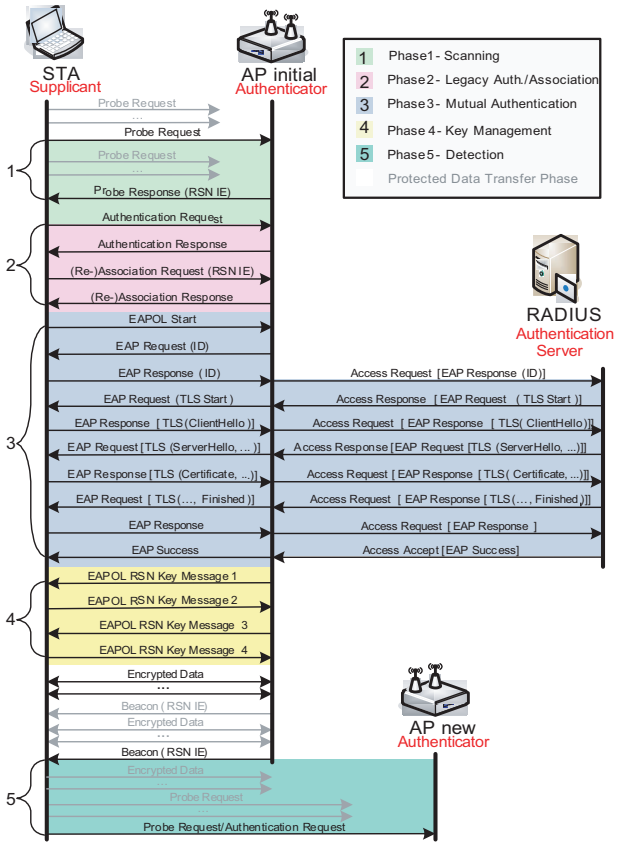

Fig. 4. RSN Phases and Message Flow

support for IEEE 802.11, is the Detection Phase. It covers the period from the last frame addressed to the STA and delivered by the initially connected AP, up to either the Probe Request or, as the case may be, the Authentication Request addressed to the new AP.

B. Testbed Configuration

With respect to the concrete experimental proceeding, two different mobile scenarios were defined. The first scenario covers an initial connection setup of an access demanding STA seeking to join an 802.11i secured wireless network which actually comprises phases 1 to 4. In this case only one AP is operating on one of the dedicated wireless medium channels in the 2.4 GHz frequency band and in IEEE 802.11b operating mode. The second scenario reflects an intra-subnet handover performed by a STA between two adjacent APs. Operating channels of both APs under study are chosen with minimal contention with neighbourhooding APs, providing rather unrealistic but optimal wireless enviroment.

After initially connecting the STA to one of the APs (while both APs are operating simultaneously each on its assigned channel) and allowing for Pre-Authentication accomplishment, the handover situation was enforced by abruptly switching off the AP which the STA has currently been connected to. In doing so, a situation was emulated when adverse conditions make for an abrupt connection loss which is, to all intents and purposes, a common scenario in present-day wireless

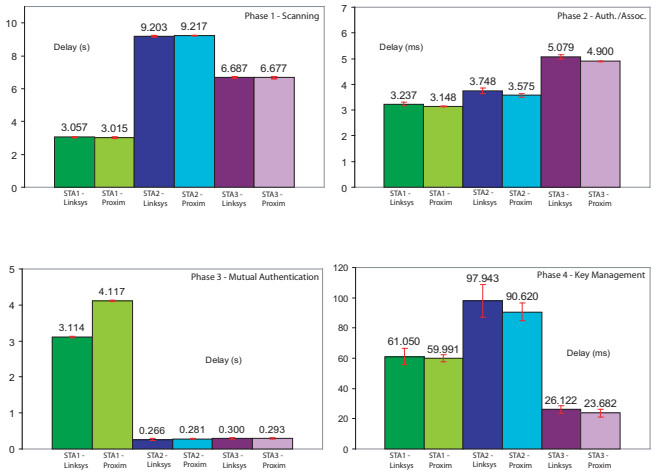

Fig. 5. Latency of Phases within Scenario 1

networks (until the standardization process of IEEE 802.11r for fast BSS transition is finalized). In this case the STA has to run through phases 1 to 5. More precisely, the measurement spans the complete period of time beginning with the detection of the need to perform a handover covered by phase 5 and ending with the establishment of an RSN security association concluded in phase 4.

Table I shows the technical specifications of the mobile clients utilized for the measurement. Those three instances give an appropriate representative cross section of commonly used mobile clients. As it is still a matter of fact that vendor specific driver implementation is a key factor in terms of performance and compliance issues, all network devices were equipped with the newest stable releases of hardware and software drivers available at the time of examination accomplishment. Furthermore, two prevalent APs as authenticators were selected, Proxim AP-4000 (approx. 300 USD) and Linksys WRT54g (approx. 60 USD). These APs provide a rough estimate on the contingent discrepancy in respect of cost/performance ratio between expensive professional equipment and rather affordable devices dedicated for residential use. The IEEE 802.11i RSN infrastructure was implemented with an Authentication Server running Ubuntu 6.06, Kernel v.2.6.15 and FreeRADIUS v.1.1.0. The infrastructure under test was the same as the one shown in Figure 3.

For each measurement configuration in turn 15 instances of the first scenario and 8 instances of the second scenario were accomplished and separately evaluated (with confidence level of 99%).

IV. Measurement Results and Analysis

A. Scenario 1: Joining the RSN Network

Considering the results of the initial RSNSA setup scenario depicted by Figure 5, it can be assessed that (active) scanning is definitely the most time consuming phase, as far as STA_2 ($\approx$ 9 s) and STA_3 ($\approx$ 6 s) are concerned.

While STA_1 transmits its Probe Request frame on the AP's frequency channel only once, the STA_2 prefers to send it

Client Name	STA_1	STA_2	STA_3
Device Type	AMD Turion64, 1.8 GHz	PIII, Intel, 850 MHz	PocketPC, Intel, 400 MHz
OS	Windows XP	Ubuntu 6.06, Kernel 2.6.15	Windows Mobile 2003
WLAN Adapter	Internal, Ralink,11a/b/g	External, Proxim ORiNOCO 11a/b/g	External, SDIO, Go WiFi E300, b/g
WPA2 Software	wpa_supplicant v0.4.9, NDIS v5.1	wpa_supplicant v0.4.8, MadWiFi	Odyssey Client v4.05

TABLE I
MOBILE CLIENTS (STAS)

thrice, two at the beginning and the third at the end of the $\approx$ 9 s scanning period. On the other hand, STA_1 and STA_3 send out their Probe Requests as Broadcast frames, although all STAs are configured to announce the SSID of the network they desire to connect to within their Probe Requests. Both, STA_1 and STA_2 have rather high scanning delay due to the active scanning on all available frequency channels.

However, as the 802.11 specification does not stipulate how scanning should actually be accomplished, the network discovery procedure is up to the implementer and thus, those remarkable differences presented above are indisputably due to vendor specific interpretation of the scanning procedure implemented by the network driver.

In contrast to the Authentication and Association Phase, delays that emerge in the measurement results of the Mutual Authentication Phase, are considerably higher especially when it comes to STA_1, which needs up to $\approx$ 4 s to carry out the EAP-TLS authentication. Actually, the TLS handshake itself is performed within $\approx$ 300 ms which is comparable to the not significantly different results of the other two STAs. However, the STA_1 supplicant defers the initiation of the authentication method by not responding to the Identity Requests sent by the APs in vain. Instead, the supplicant seems eager to commence the authentication process all by itself in virtue of transmitting an EAPOL Start frame. This inflexibility, which actually is not conformant to the 802.11i security standard has a high price and lets STA_1 gravely narrow its lead over the other two STAs in terms of overall connection delay.

Contemplating on the delay times of the Key Management Phase, a phase which executes a 4-Way Handshake, a significant difference between all three systems is in evidence. Although the STA_1 device is in terms of hardware power superior to STA_2 or STA_3, it evidently does no make profitable use of the available resources and consequently, let the weakest device outperform the actually more sophisticated ones.

In order to resume all four phases at a glance as parts of the first scenario (RSNSA setup scenario), Figure 6 is meant to illustrate the complete scenario summary.

B. Scenario 2: Handover within RSN Networks

Having discussed the characteristics of the three examined STAs with regard to the initial RSNSA setup, it is to ascertain in how far Pre-Authentication and PMKSA Caching are capable of advancing performance issues and whether they are supported by currently deployed network equipment at all.

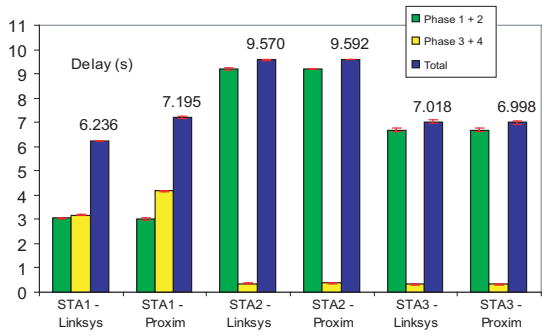

Fig. 6. Scenario 1: Results Summary

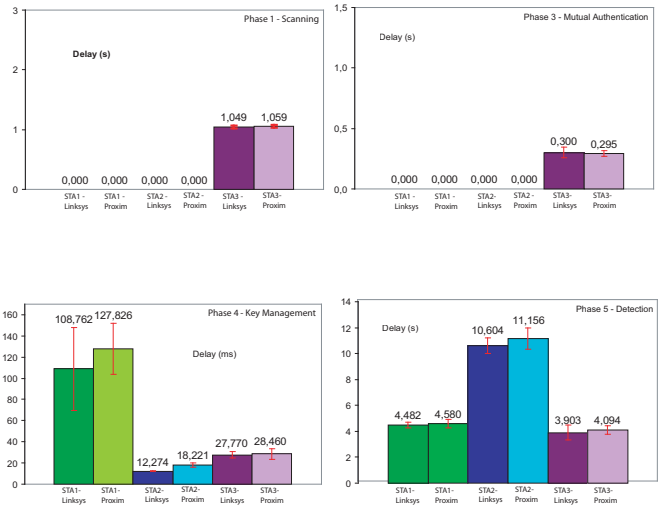

Fig. 7. Latency of Phases within Handover RSNSA Scenario

Now, taking Figure 7 into account which depicts the results of the handover scenario, the Scanning Phase, which has been considered the biggest part of the connection delay overhead as yet, now is accomplished in advance when STA_1/STA_2 initially connects to the network. The STA_3 actually would have to rescan the entire wireless environment for $\approx$6 s again, but being already connected to the network, its scanning delay decreases to only $\approx$1 s. This implementation specific feature which decreases scanning delay by selectively searching for the network with the same ESSID as a previous one strongly

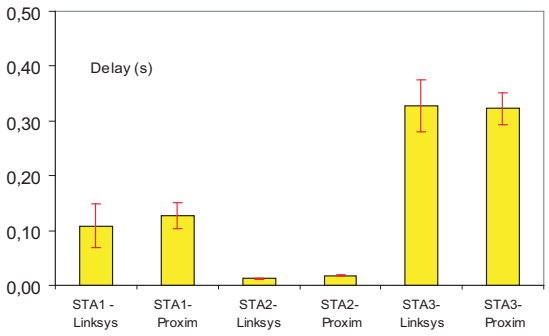

Fig. 8. Authentication Latency (without detection) within Handover Scenario

reduces the overall connection delay in spite of no support for Pre-Authentication or PMKSA Caching.

The Mutual Authentication Phase from Figure 7 shows that STA_1 and STA_2 take the advantage of using Pre-Authentication and PMKSA Caching. Both accomplish this phase in advance when initially connecting to the network and fully avoid any delay, whereas STA_3 has to perform the authentication as usually leaving him with $\approx$ 300 ms delay. On the other hand, the Key Management Phase in turn is obligatory for any connecting STA and is not significantly different from the first scenario.

The Detection Phase which provides information about how quickly a STA is able to detect an abrupt connection loss and to initiate a new connection setup. Whereas STA_1 and STA_3 need $\approx$ 4 s to perform this action, Linux-STA hangs in the balance up to $\approx$ 12 s without any connection to the network. Also, its average values are highly significantly different from the ones of the other STAs.

Summarizing the entire procedure (as per Figure 8), it is obvious that the authentication latency is highly device and implementation dependent. Now, granted that STAs would be able to perform a handover without having to detect a loss of connection (which is the objective of 802.11r "fast roaming" Task Group), the results show that the actual process of reconnecting to the network takes at worst about 172 ms for STA_1, about 27 ms for STA_2 and about 1.422 s in the case of STA_3. Only in the case of STA_3, which requires about 300 ms on passing through another Mutual Authentication Phase, both other systems make themselves avail of their enhanced Pre-Authnentication and Key Caching capabilities. As a result, an overall authentication delay for STA_1 and STA_2 is $\approx$ 110 ms and $\approx$19 ms, respectively. STA_3 without utilizing pre-authentication and key caching reaches authentication delay of $\approx$ 330 ms. This high variance of presented results shows that the implementation of the security standard still leaves much room for improving but also impairing the overall latency. It also shows that pre-authentication and key caching are important latency-decreasing techniques which should be implemented by every mobile device.

V. Conclusion

This work allows for a pragmatic view on today's secure alleged wireless networks which are expected not only to provide sophisticated secure data transfer but also to be effortlessly integrated with other application domains like the forthcoming Voice over WLAN (VoWLAN). In this context, there has been a need of elaborating on how far IEEE 802.11i is capable of improving existent shortcomings but also to get an insight into the maturity of today's devices. Although the scanning delay and detection delay have a major effect on overall delay, they both are still a subject of standardization within IEEE Task Group "r". The first draft of IEEE 802.11r is expected in 2007, and it can be assumed that scanning and detection delays are subject to optimization. On the other hand, the 802.11i security standard has recently been ratified, leaving less room for improvement. This could change the overall landscape of latencies within 802.11i secured networks, making the latency caused by security a major challenge for competitive implementations. As a result, this could have a further impact on the overall deployment of secure wireless networks. It would not be the first time to see security being turned off for better performance, even if problems with the latter is only a matter of implementation.

References

[1] IEEE 802.11. IEEE Standard for Local and Metropolitan Area Networks - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Standard, July 1999.

[2] IEEE 802.11i/D10.0. Security Enhancements, Amendment 6 to IEEE Standard for Information Technology. IEEE Standard, April 2004.

[3] IEEE 802.1X. IEEE Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control. IEEE Standard, June 2001.

[4] B. Aboba and P. Calhoun. RADIUS Support For Extensible Authentication Protocol (EAP). RFC 3579, 2003.

[5] T. Dierks and C. Allen. The TLS Protocol Version 1.0. RFC 2246, 1999.

[6] H. Duong, A. Dadej, and S. Gordon. Proactive Context Transfer and Forced Handover in IEEE 802.11 Wireless LAN based Access Networks. *SIGMOBILE Mob. Comput. Commun. Rev.*, 9(3):32–44, 2005.

[7] M. Kassab, A. Belghith, J.-M. Bonnin, and S. Sassi. Fast Pre-authentication based on Proactive Key Distribution for 802.11 Infrastructure Networks. In *WMuNeP '05: Proceedings of the 1st ACM workshop on Wireless Multimedia Networking and Performance Modeling*, pages 46–53. ACM Press, 2005.

[8] I. Martinovic, F. A. Zdarsky, A. Bachorek, C. Jung, and J. B. Schmitt. Phishing in the Wireless: Implementation and Analysis. In *Proceedings of the 22nd IFIP International Information Security Conference (SEC 2007), Johannesburg, South Africa*, May 2007.

[9] I. Martinovic, F. A. Zdarsky, A. Bachorek, and J. B. Schmitt. Introduction of IEEE 802.11i and Measuring its Security vs. Performance Tradeoff. Technical Report 35106, University of Kaiserslautern, Computer Science, Kaiserslautern, Germany, September 2006.

[10] D. Mills. Network Time Protocol v.3 Specification, Implementation and Analysis. RFC 1305, 1992.

[11] A. Mishra, M. Shin, and W. Arbaugh. An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process. *SIGCOMM Comput. Commun. Rev.*, 33(2):93–102, 2003.

[12] A. Mishra, M. Shin, and W. Arbaugh. Context Caching using Neighbor Graphs for Fast Handoffs in a Wireless Network. *Proceedings of the IEEE INFOCOM Conference*, pages 361–372, March 2004.

[13] I. Ramani and S. Savage. SyncScan: Practical Fast Handoff for 802.11 Infrastructure Networks. *Proceedings of the IEEE INFOCOM Conference*, March 2005.

[14] H. Velayos and G. Karlsson. Techniques to Reduce IEEE 802.11b MAC Layer Handover Time. Technical Report TRITA-IMIT-LCN R 03:02, KTH, Royal Institue of Technology, Stockholm, Sweden, April 2003.