Introduction of IEEE 802.11i and Measuring its Security vs. Performance Tradeoff

Technical Report No. 351/06

Ivan Martinovic, Frank A. Zdarsky, Adam Bachorek, and Jens B. Schmitt

disco | Distributed Computer Systems Lab
University of Kaiserslautern, 67655 Kaiserslautern, Germany

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 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 at least in the former case poses a problem as far as meeting quality of service demands of the forthcoming applications (e.g. Voice over WLAN).
Main objective of this empirical research is to reveal how currently deployed mobile computer systems perform when joining such a robust and secure network as defined by the IEEE 802.11i security amendment. Particularly mobile handover scenarios are supposed to be regarded as a critical issue which is imperative to be dwelled on in measurements and appropriate analysis covered by this paper. In this context, the entire network connection process of an admission demanding mobile station is being resolved into its particular phases and analyzed. Furthermore, there has been a need of elaborating on the underlying issue in how far 802.11i is capable of improving this definite shortcoming by making use of Pre-authentication and Key Caching and thus keeping up the chance to become the ultimate security standard for future markets.

Keywords:
WLAN, Security, IEEE 802.11i

1 Introduction

Ever since IEEE 802.11 became the first widely-approved wireless networking standard, Wireless Local Area Networks (WLANs) have exhibited significant growth regarding corporate as well as home networking environments. Nowadays, 802.11-based networks enjoy immense popularity in the ever-growing communication and information society at such a rate that they seem to be ubiquitous in our every day life. Airports, coffee shops and campuses represent Hot Spot areas where mobile access to the world's overarching Internetwork is granted. A high percentage of all present-day enterprises equip their staff with mobile

devices allowing for the ability to carry out their tasks while being en route on the premises. This in turn results in increase in productivity and as a rule it leads to a sophisticated corporate culture.

The most remarkable benefit of WLANs in this regard is their provision of much higher transmission rates of up to 108 Mbps at tolerable costs which is significantly more than e.g. third generation cellular mobile systems like the Universal Mobile Telecommunications System (UMTS) are able to offer. Yet security in wireless networks is a serious concern when considering the matter of fact that communication through air as the wireless carrier medium for personal and business data can easily encounter attacks such as eavesdropping, masquerading or denial-of-service. Based upon the ease of intercepting and injecting network communication, those are severe threats which not only violate privacy but also might pose a certain amount of risk for business or even national affairs.

While in the course of time legacy IEEE 802.11 [1] security conception shaped up as somewhat of a letdown when more and more deficiencies were disclosed, many vendors tried to overcome this drawback by means of extending their conformant implementations by proprietary security features. Yet a weak encryption algorithm, no proper integrity check and a replayable authentication method amongst others were the proximate cause for the failure of the legacy security features known collectively as Wired Equivalent Privacy (WEP) to ensure the support of fundamental security objectives like confidentiality and access control [8].

Facing the dispersion of proprietary solutions which would undisputedly lead to a decreasing interoperability of wireless devices an industry consortium of WLAN equipment vendors called the Wireless Fidelity (Wi-Fi) Alliance attended to this issue and founded an interoperability certification program for IEEE 802.11 conformant products in 2002. Based upon a subset of concepts and security requirements established by the Institute of Electrical and Electronics Engineers (IEEE) for the officially aspired IEEE 802.11i security amendment, the Wi-Fi certification program was merely intended as an interim solution introducing the so-called Wi-Fi Protected Access (WPA) industry standard. WPA-certified equipment was supposed to meet advanced security requirements such as stronger encryption and integrity verification by means of an elaborate cryptographic method known as Temporal Key Integrity Protocol (TKIP) as well as trustworthy user authentication and efficient key management with the aid of the IEEE 802.1x authentication and authorization framework for IEEE 802.1 networks. In either case, legacy-based devices ought to be effortlessly upgraded in order to acquire the WPA-certification e.g. in virtue of a software update instead of a costly hardware replacement [9,10].

The anticipated ultimate solution to the hitherto existing security inadequacies was finally presented in 2004 when the IEEE successfully ceased its 802.11i ratification endeavors [2]. The cornerstone of this sixth amendment to the baseline IEEE 802.11 standards is the concept of a separation of the user authentication and the message protection process which allows for embedding many currently stationary-approved authentication protocols like Kerberos and Exten-

sible Authentication Protocol (EAP) [4] over Transport Layer Security (TLS) [6] into the wireless networking domain. Another groundbreaking amelioration in 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) [2]. 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 into account the Wi-Fi Alliance released the WPA2 certification program in the end of 2004 in order to carry on accounting for product interoperability of any vendor.

All things considered, IEEE 802.11i offers a quite complete security suite to satisfactorily accomplish advanced security objectives in wireless networks provided that all featured mechanisms collaborate in a proper way. Nevertheless, it should be quite evident that such substantial enhancements involve additional processing complexity and communication between participating network entities which in turn results in collateral time consumption. To what extent this time overhead affects the entire connection setup process of wireless stations attempting to access the network and in how far amendatory standard features like pre-authentication in conjunction with key caching are able to produce relief in this matter is part and parcel of the work in hand. More precisely, it is to clarify whether wireless stations are able to adhere to the strict quality of service requirements of time critical applications like the forthcoming Voice over WLAN (VoWLAN) especially when it comes to mobile scenarios, and handoffs between adjacent access points within the same subnet domain become inevitable. Figure1 exemplarily illustrates such a setting within a typical enterprise network topology.

In this spirit, the intended contribution to the state-of-the-art in the area of wireless security presented in this work is twofold. First, an empirical examination is meant to accent the impact of 802.11i security mechanisms in terms of communication overhead caused by auxiliary frame exchange between a wireless station and the corresponding network components within the network distribution system. This examination had been conducted in realistic mobile scenarios including an initial secure connection setup as well as a layer 2 intra-handover within an established RSN. Analyzing each piece of the partly secured network connection process performed by an access demanding mobile wireless station provided detailed information about overhead distribution and particularly the additional time consumption as far as the 802.11i security amendment is concerned. Second, for each series of measurements three entirely different computer systems were used similarly in the role of an access demanding client which is also referred to as the supplicant. These systems differed in their running operating system, their wireless network interface as well as their hardware configuration and specification details. This diversity allows for identifying certain aspects of security provisioning in present-day wireless networks which haven't been addressed in such a manner yet.

In fact, divulging these results as per particulars given in section contributes to the awareness of what public can expect from current network-enabled computer systems which are obtainable anywhere and even affordable these days.

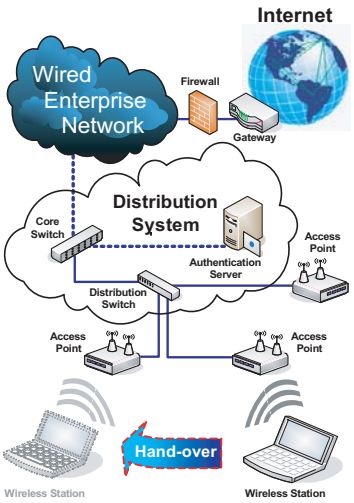

Fig. 1. Layer 2 Handover

The remainder of this paper is organized as follows. Section 2 provides a brief insight into the 802.11i standard. The related work on this subject is discussed in Section 3. The main part of this research consisting of Section 4 and its subsections examines common 802.11i wireless network in a mobile handover scenario. Section 5 concludes the paper summarizing the results of the measurement campaign.

2 IEEE 802.11i in a Nutshell

After motivating the ongoing topic and introducing the scope of this paper it is essential to take a closer look at the elementary security mechanisms of the IEEE 802.11i standard which are considered to be the ultimate improvements of the legacy security endeavors. This allows for creating a basis for further discussion and deeper comprehension of what really makes up a robust and secure network, to what extent those security mechanisms have an impact on connection delay and in how far the standard in question already features the needed methods to counter the consequences of intra-subnet hand-overs in wireless secure networks.

The quintessence of the IEEE 802.11i specification is the concept of a Robust Secure Network [2]. 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 which defines the basis model for the support of authentication services such as enhanced mutual authentication and key management via EAP. Moreover, they also offer confidentiality and data integrity by means of two cryptographic methods called CCMP and TKIP. In order to impart an adequate knowledge of that security framework the succeeding subsections resume the key issues of its components.

2.1 Port-based Network Access Control

The IEEE 802.1X [3] specification defines a general framework for the provision of authentication services by means of the port-based access control mechanism. This model includes three fundamental components which are related to those services each in a different way. Usually as part of the distribution system the Authentication Server (AS) is the network element which provides the authentication service to an entity defined as the authenticator through the back-end of the network system. A supplicant, in this context, is a network component that shares a wired or wireless point-to-point link with the authenticator and seeks to be authenticated by the means of that authentication service. In order to be authorized to access the services provided by the authenticator, the supplicant's credentials need to be validated against the information hold by that authentication service.

Now mapping this model to the semantics of a wireless RSN as per IEEE 802.11i and let the roles of authenticator and supplicant be adopted by an access point (AP) and a wireless station (STA) respectively, the port-based access mechanism may be briefly elucidated as follows. The AP holds two communication ports, an uncontrolled authentication port and a controlled service port (see Figure). As long as the authentication process including the key management between the STA and the AS has not yet finished successfully, the AP only permits authentication-related traffic via its uncontrolled port and blocks any other traffic on the controlled port prohibiting access to WLAN resources and services the network provides. Once the authentication and key management phase is completed the authenticated STA is granted access to the network via the controlled service port of the AP.

Commonly used and recommended protocols for the authentication process are EAP and the Authentication Dial In User Service (RADIUS) protocol. While EAP encapsulates the messages of any suitable higher layer authentication method between the STA and the AP, the RADIUS protocol on its part attends to encapsulation of the EAP method's message exchange between the AP and the AS. The combination of both protocols provides for (mutual) authentication between the STA and the AS while the AP rather acts as passive broker forwarding messages via its uncontrolled authentication port from STA to AS and vice versa. Figure 2 illustrates a RSN environment as per IEEE 802.11i as well as the IEEE 802.1X port-based network access control mechanism.

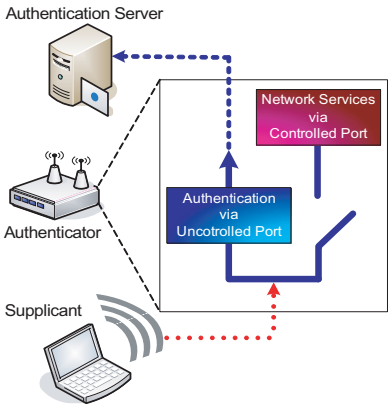

Fig. 2. IEEE 802.1X port-based network access

2.2 Mutual Authentication

As already stated in the preface of this section a RSNA relies on IEEE 802.1X port-based access control mechanism to provide for authentication services whereas the Extensible Authentication Protocol (EAP) represents the flexible authentication framework which can be adapted to a wide variety of authentication methods. While EAP defines the general packet formats and message types utilized to encapsulate the concrete authentication procedure, EAP methods on their part perform the authentication transaction and are responsible for the procurement of the necessary key material used to cryptographically protect subsequent data exchange and thus grant a confidential and authentic communication.

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 away from the encapsulated authentication method and enables the AP to forward authentication messages between the STA and the authentication infrastructure in the back-end of the network, typically consisting of a unique RADIUS Server (RS). Figure 3 depicts the three-part message flow of 802.1X/EAP in conjunction with RADIUS/EAP as the carrier protocols for specific authentication methods.

In the first part, the user identity of the STA is requested by the AP and the response is forwarded to the AS, which is supposed to validate this identity against an existent user account defining available methods and credentials needed to proceed with the authentication process. This authentication phase may be initiated either by the STA sending an EAP over LAN (EAPOL) Start frame prior to a Request Identity frame or alternatively by the AP sending the

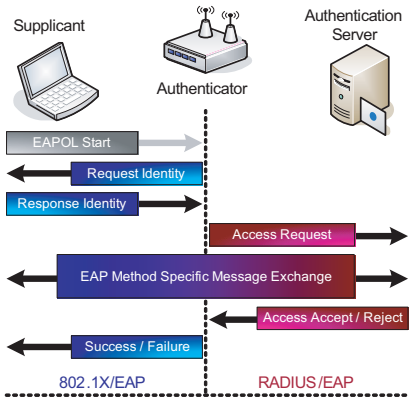

Fig. 3. EAP authentication message flow

Request Identity message immediately. In the second part, the actual authentication method (as defined for the user account) is initiated by the AS. Henceforth, any message of the chosen authentication method is encapsulated within EAP-Request/-Response frames on the STA's and within RADIUS Request/-Challenge frames and bidirectional forwarded by the AP between the STA and the AS. When the authentication method finishes its message exchange, the AS transmits an EAP-Success or EAP-Failure message to the STA via the AP depending on whether the authentication was successful or not respectively [5].

As the 802.11i standard doesn't commit to specify which particular authentication method to employ when implementing a 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 in hand shall rather focus on the for most commonly used and universally approved authentication method known as Transport Layer Security (TLS).

TLS is considered the most secure of the EAP methods because of a strong cryptographic background through the use of public key certificates. Also, it is one of the only five EAP methods currently comprised in the WPA2 certification program of the Wi-Fi Alliance and while being widely deployed by numerous WLAN vendors, EAP-TLS has finally emerged as the dominant authentication protocol for trusted IEEE 802.11i RSN support. In the first instance, it benefits from it resistance against man-in-the-middle and dictionary attacks as well as its support for protected cipher suite negotiation, mutual authentication and session key derivation.

Assuming that there is a trusted CA which issued a signed client certificate to the STA as well as a signed server certificate to the AS, a TLS session handshake typically proceeds in the following manner (as per illustrated in Figure 4).

The client STA initiates the TLS session handshake by sending a ClientHello message containing a random number N1 and a list of supported cipher suites to the AS. The ServerHello response message sent by the AS includes its ServerCertificate, another random number N2, the chosen cipher suite and the CertificateRequest demanding the STA's certificate to be included in the subsequent client message in order to provide for mutual authentication.

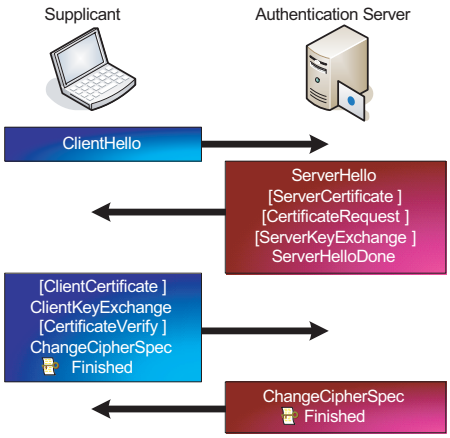

Fig. 4. TLS Handshake

Depending on the session key negotiation method the AS may also send a ServerKeyExchange message element containing additional key negotiation data. The ServerHelloDone message element is just a notification for the client that no further optional message elements will be sent by the AS. The client STA is now able to verify the ServerCertificate using the CA's public key. If the signature is valid, then the client STA can find the authentic public key of the AS in its transmitted ServerCertificate and use it to encrypt another random value N3 henceforth pre-master secret. The asked for ClientCertificate, the encrypted pre-master secret and the CertificateVerify message as the digital signature of the handshake messages signed by the client STA's private key are the elements included in the subsequent message sent by the client STA. By means of the CertificateVerify the STA can prove that it owns the appropriate private key corresponding to the public key contained in its ClientCertificate. Computing the hashed value of the two random numbers N1, N2 and the pre-master secret, the STA and the AS are able to derive the shared session key. The ChangeCipherSpec message element acknowledges the negotiated cipher suite to be applied to all subsequent messages sent by the client STA. The first data protected by this cipher suite is the Finished message element. The AS ceases the TLS session handshake by sending a last message including the ChangeCipherSpec and Finished message element, the latter as the first data

protected by the negotiated cipher suite on the part of the AS and including a hashed value of the handshake messages as well as the pre-master secret which allows for authenticating the AS.

2.3 Key Management

Generally speaking, security provisioning is fundamentally based upon secret keys. In RSN environments all keys have a limited lifetime and are organized in a key hierarchy (see Figure 5).

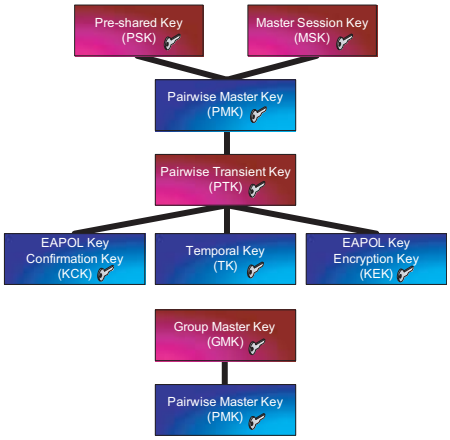

Fig. 5. RSN Key Hierarchy

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 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 temporal Group Transient 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 6).

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.

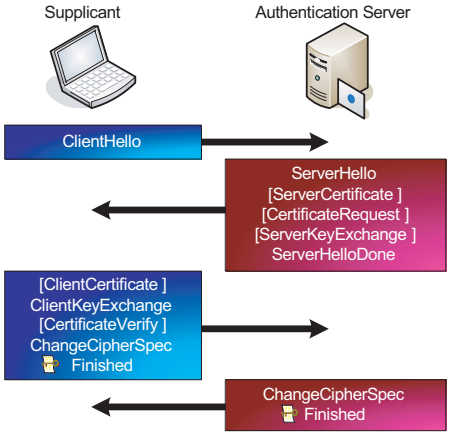

Fig. 6. 4-Way Handshake message flow

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.

2.4 Confidentiality and Integrity

Now that the STA has successfully completed the mutual authentication as well as key management phase, it is supposed to make use of the derived TK to secure the wireless communication with the corresponding AP. The TK as the shared secret and one of the inputs to cryptographic algorithms is the key factor of secure data transfer.

The two main purposes of applying cryptographic encryption schemes is to ensure confidentiality and data integrity, in other words, to protect data against unauthorized disclosure and to validate the data originator while preventing data from being tampered respectively. In order to allow for accomplishment of these two objectives the 802.11i security amendment includes two corresponding cipher suites TKIP and CCMP. Because support of the former is merely classified as optional by the standard, it shall suffice to solely throw a glance at the latter and more sophisticated one. Also, CCMP as the mandatory cipher suite for RSN-conformant network environments is far less vulnerable to attacks than TKIP and therefore the recommended choice in terms of robust security establishment in business and advanced private wireless networks.

CCMP is based on a generic encryption block cipher mode of AES and uses a single 128-bit cryptographic key (which is the TK) for both encryption and integrity protection. As per specification the TK is a per session key which means it is valid for the entire duration of a station-to-AP association. These features along with the pre-computation of certain cryptographic parameters allows for a reduced complexity and thus overhead decimation. Besides, the cryptographic scheme of CCMP includes integrity protection of the packet payload as well as of a portion of the packet header by means of a Cipher Block Chaining Message Authentication Code (CBC-MAC). Replay attack resistance is guaranteed by a 48-bit packet number which is used as an initialization vector for the cryptographic algorithm and included in the CCMP part of the frame header. Incrementing the

packet counter by one with every encrypted frame lets the TK outlive any conceivable association period and thus limits the need to renew the TK to adverse conditions like the compromise of any credentials. In short, CCMP represents a high level and surpassing security scheme which is considered as central to the RSN provisioning of confidentiality and data authenticity.

2.5 Pre-Authentication and PMK Caching

In addition to the sought-after 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. The mechanisms in question 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 hand-overs and in how far these amendatory mechanisms are already included in currently available implementations. For this shall not be assumed as a matter of course.

Now that a sufficient review of the IEEE 802.11i security amendment and further details related to the scope of this work are complete, readers are given a solid comprehension basis and the required terminology to be better able to unambiguously relate to the following discussion, examination and analysis.

3 Related work

Much research has been devoted to the analysis of network discovery in local wireless networks which still poses a grave problem to applications insisting on upper delay bounds. Attending to this issue, empirical studies in [15,12,14] 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 [15] and [12], 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 [15] 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. In [13] 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) which tries to circumvent the Mutual Authentication Phase of the 802.11i approach is covered by [7]. 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 [11]. In virtue of two additional methods the solution in [11] seeks to exclude the key management phase from the overall connection process. The first technique enables a STA to accomplish the 4-Way-Handshake with all adjacent APs immediately after connecting to the network so as to preclude another key exchange in handover scenarios. In contrast, the second technique makes arrangements to make up for the 4-Way-Handshake ex post, i.e. after the handover maneuver.

Nevertheless, none of these works incorporated an overall view of the entire network connection process but rather singled out just one or more parts in order to develop and apply their own suggestion for improvement. A further difference to our study is that the impact of Pre-authentication and PMK Caching has not yet been analyzed. In fact, this circumstance warrants the subsequent experimental proceeding of taking every single connection phase into account as pointed out in this paper.

4 Examination of a Mobile 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.

4.1 RSN Connection Process Overview

Summarizing at a glance all the mechanisms introduced in the section 2, this introductory subsection is meant to dwell on the complete RSN connection process which allows for getting a concrete idea of the communication and message exchange of RSN components within an enterprise or advanced private network environment.

Basically, the act of (re-)connecting to any kind of wireless networks consists of a sequence of successive phases, each with a different purpose. Dividing the entire 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 7. The first phase corresponds to the active or passive network discovery procedure (henceforth Scanning Phase) of a mobile station seeking to find appropriate network access points. Here, a STA either passively scans the wireless medium for beacon frames periodically transmitted by APs, or it actively sends Probe Request frames requesting nearby APs to answer with Probe Responses. Both AP messages are expected to comprise the so called RSN Information Element (RSN IE), which announces the AP's RSN capabilities in 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 on its part 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. Again, the RSN IE embedded in the STA's (Re-) Association Request frame provides information about its capabilities and serves as the means by which the AP decides on acceptance or rejection of the STA's admission request depending on whether it meets the network's security critical stipulations. As already mentioned, this paper focuses on the EAP-TLS combination as a highly secure and well understood authentication method. Therefore, phase number three 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.

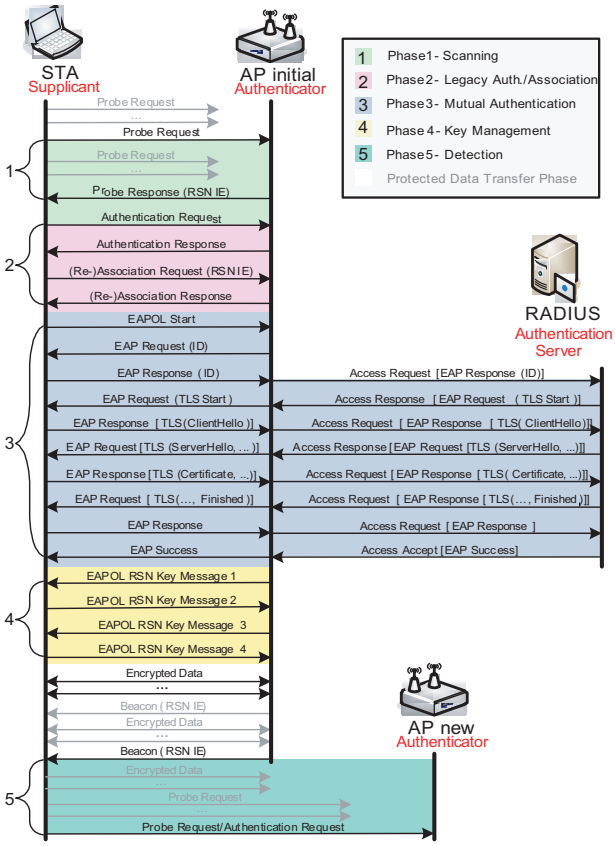

Fig. 7. RSN phases and message flow

At last, the Key Management Phase concludes the RSNSA establishment process. 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 received by the STA. Hereupon the protected Data Transfer Phase begins allowing for secure and authenticated message delivery and receipt. While this part is not relevant to the conducted empirical survey, there is another phase of the connection process which is worthwhile a deeper study especially when it comes to hand-over situations. It is the Detection Phase which 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 AP the STA

is up to joining. On the one hand, this predefinition of the phase boundaries is determined by the experimental proceeding discussed in the next subsection and, on the other hand, it depends on the capabilities of the supplicant implementation installed on the examined device.

4.2 Measurements

With regard to the concrete experimental proceeding, two different mobile scenarios were defined implicating a STA's passing through 4 and 5, respectively, of the phases introduced in the previous subsection. The first scenario covers an initial connection setup of an access demanding STA seeking to connect to 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 being channel 1 and channel 6, respectively. The second scenario reflects an intra-subnet hand-over maneuver performed by a STA between two adjacent APs. As the simulation of mobility by means of manually moving a STA from one AP cell to the other would definitely involve several influencing factors gratuitously complicating the proximate evaluation and thus constricting the comparability of device configurations, the actual scenario was realized in the following manner. 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 hand-over situation was enforced by abruptly switching off the AP which the STA is currently connected to. In doing so, a situation was simulated when adverse conditions make for a abrupt connection loss which is, to all intents and purposes, a common scenario in present-day wireless networks. In this case the STA has to run through phases 1 to 5. More precisely, the measurement capture has to span the complete period of time beginning with the detection of the need to perform a hand-over covered by phase 5 and ending with the establishment of a RSN security association concluded in phase 4 in order to incorporate the implementation specific behavior of the STA in this kind of mobile scenario.

Client Name	WinXP	Linux	WinM
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,11b/g	External, Proxim ORiNOCO 11b/g	External, SDIO, Go WiFi E300
WPA2 Software	wpa_supplicant v0.4.9, NDIS v5.1	wpa_supplicant v0.4.8, MadWiFi	Odyssey Client v4.05

Table 1. Mobile Clients (STAs)

As per commonly used convention a measurement configuration defines a certain state of the measurement environment including the hardware and software settings of each component. For each measurement configuration in turn 15 measurement instances of the first scenario and 8 instances of the second scenario were accomplished and separately evaluated (with confidance level of 99%). Moreover, during any measuring process all activities on the currently occupied wireless channels were captured by a purpose-configured mobile station equipped with two wireless network adapters. In fact, this capability allows for simultaneous capturing on two different wireless channels at all which is the quintessence for a precise investigation of real-world mobile scenarios including roaming from one wireless channel to another.

As one of the crucial points, this paper intends to provide for an authentic state-of-the-art overview of the impact of 802.11i security enhancements on the overall communication delay due to auxiliary protocol overhead in conjunction with mobility aspects. In this context, it seeks to emphasize the relevance of different device specifications by showing in how far they may imply different measurement results. To this end a test bed environment was established which reflected a realistic RSN deployment and provided the platform by which mobile scenario simulations were made feasible. Table 1 tabulate the technical specifications of the network entities utilized for the measurement campaign. Attention should be paid to the diversity in hardware and software specifications of the selected mobile stations. Those three instances give an appropriate representative cross section of commonly used network enabled mobile computer systems. 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 were selected, differing primarily in the matter of expense, so as to provide for a rough estimate on the contingent discrepancy in respect of cost/performance ratio between expensive professional equipment and rather affordable devices dedicated for domestic 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.

4.3 Results

Considering the results of the initial RSNSA setup scenario depicted by Figure 8, it can be assessed that (active) scanning is definitely the most time consuming phase, as far as Linux ($\approx$ 9 s) and WinM ($\approx$ 6 s) are concerned.

While WinXP transmits its Probe Request frame on the AP's frequency channel only once, the Linux system prefers to send it thrice, two at the beginning and the third at the end of the $\approx$ 9 s scanning period. On the other hand, WinXP and WinM 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. However, as the 802.11 specification does

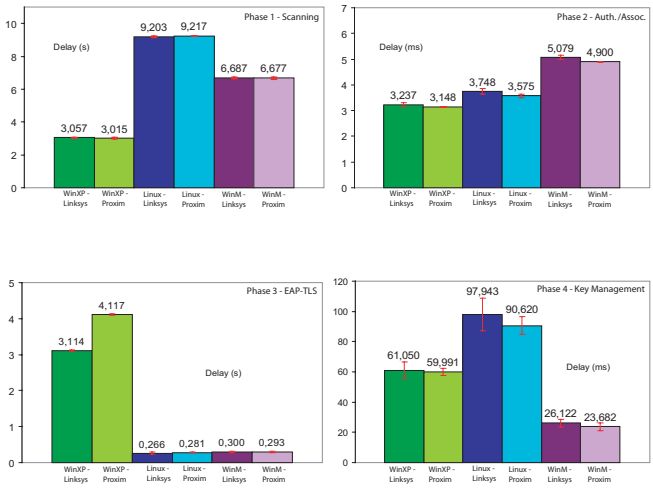

Fig. 8. Latency of Phases within Initial RSNSA Scenario

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 WinXP, which needs up to ≈ 4 s to carry out the EAP-TLS authentication. Actually, the TLS handshake itself is performed within ≈ 300 ms which is comparable to the not significantly different results of the other two STAs. However, the WinXP 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 WinXP 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 WinXP device is in terms of hardware power superior to Linux or WinM, it evidently does no make profitable use of the available resources and consequently, let the weakest devise outperform the actually more sophisticated ones.

In order to resume all four phases at a glance as parts of the initial RSNSA setup scenario, Figure 9 is meant to illustrate the complete scenario summary.

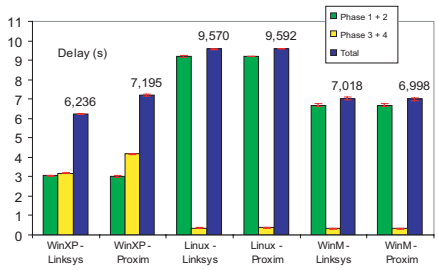

Fig. 9. Initial RSNSA Scenario Summary

As it should be apparent from that figure, the IEEE 802.11i security mechanisms (subsumed in Phase 3+4) have just a minimal impact (except for WinXP) on the overall time delay although they all exceed the delay-critical threshold of 20 ms.

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.

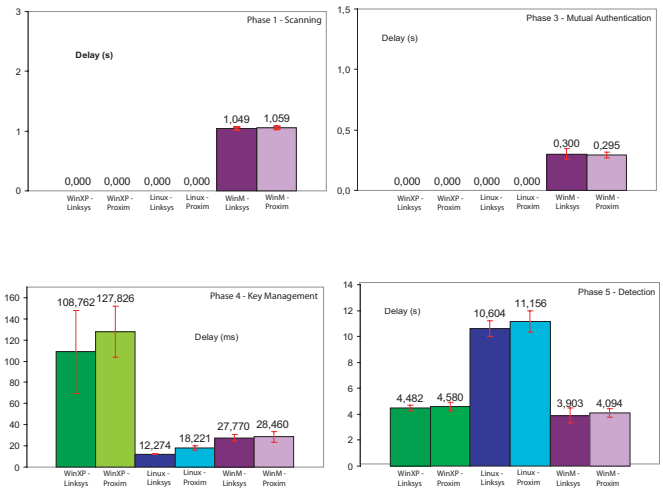

Fig. 10. Latency of Phases within Handover RSNSA Scenario

Now, taking Figure 10 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 WinXP/Linux initially connects to the network. The WinM actually would have to rescan the entire wireless environment for ≈6 s again, but being already connected to the network, its scanning delay decreases to only ≈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 reduces the overall connection delay in spite of no support for Pre-Authentication or PMKSA Caching.

The Mutual Authentication Phase from Figure 10 shows that WinXP and Linux 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 WinM has to perform the authentication as usually leaving him with ≈ 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.

Last but not least, there is 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 WinXP and WinM need ≈ 4 s to perform this action, Linux-STA hangs in the balance up to ≈ 12 s without any connection to the network. Also, its average values are highly significantly different from the ones of the other STAs.

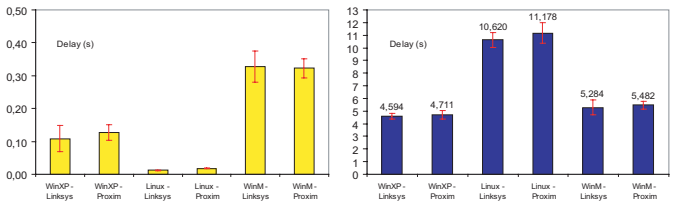

Fig. 11. Authentication and Overall Latency

Summarizing the entire procedure (as per Figure 11), it is obvious that the authentication latency has only a minor impact on the complete handover delay. But, 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 WinXP, about 27 ms for Linux-STA and about 1,422 s in the case of WinM. The high variance of the results shows that the implementation of the security standard still leaves much room for improving but also impairing the overall latency.

5 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 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, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz. Extensible Authentication Protocol (EAP). RFC 3748, 1999.
5. B. Aboba and P. Calhoun. RADIUS Support For Extensible Authentication Protocol (EAP). RFC 3579, 2003.
6. T. Dierks and C. Allen. The TLS Protocol Version 1.0. RFC 2246, 1999.
7. 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.
8. S. Fluhrer, I. Mantin, and A. Shamir. Weaknesses in the key scheduling algorithm of RC4. In *SAC '01: Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography*, pages 1–24, August 2001.
9. S. Frankel, B. Eydt, L. Owens, and K. Kent. Guide to IEEE 802.11i: Establishing Robust Security Networks. National Institute of Standards and Technology, June 2006.
10. M. Gast. *802.11 Wireless Networks: The Definitive Guide*. O'Reilly, 2005.
11. 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.

12. 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.
13. 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.
14. I. Ramani and S. Savage. SyncScan: Practical Fast Handoff for 802.11 Infrastructure Networks. *Proceedings of the IEEE INFOCOM Conference*, March 2005.
15. 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.