HAL
open science

Fast pre-authentification based on proactive key distribution for 802.11 infrastructures networks

Mohamed Kassab, Abdelfettah Belghith, Jean-Marie Bonnin, Sassi Sassi

To cite this version:

Mohamed Kassab, Abdelfettah Belghith, Jean-Marie Bonnin, Sassi Sassi. Fast pre-authentification based on proactive key distribution for 802.11 infrastructures networks. WMuNeP 2005 : first ACM workshop on wireless multimedia networking and performance modeling, Oct 2005, Montréal, Canada. pp.46 - 53. hal-02899588

HAL Id: hal-02899588

https://hal.science/hal-02899588v1

Submitted on 10 Jun 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Fast Pre-Authentication Based on Proactive Key Distribution for 802.11 Infrastructure Networks

Mohamed Kassab[1], Abdelfettah Belghith[1], Jean-Marie Bonnin[2], Sahbi Sassi[1]
[1]CRISTAL Laboratory, Ecole Nationale des Sciences de l'Informatique, Tunis, Tunisia
{Mohamed.kassab,Abdelfattah.belghith, sahbi.sassi}@ensi.rnu.tn

[2] Ecole Nationale Supérieure de Télécommunications de Bretagne, Rennes, France
Jmb.bonnin@enst-bretagne.fr

ABSTRACT
Recently, user mobility in wireless data networks is increasing because of the popularity of portable devices and the desire for voice and multimedia applications. These applications, however, require fast handoffs among base stations to maintain the quality of the connections. Re-authentication during handoff procedures causes a long handoff latency which affects the flow and service quality especially for multimedia applications. Therefore minimizing re-authentication latency is crucial in order to support real-time multimedia applications on public wireless IP networks. In this paper, we propose two fast re-authentication methods based on the predictive authentication mechanism defined by IEEE 802.11i security group. We have implemented these methods in an experimental test-bed using freeware and commodity 802.11 hardware and we demonstrate that they provide significant latency reductions compared to already proposed solutions. Conducted measurements show a very low latency not exceeding 50 ms under extreme congested network conditions.

Categories and Subject Descriptors
C.2.1 [**Computer Communication Networks**]: Network Architecture and Design – *Wireless communication.*
C.2.0 [**Computer Communication Networks**]: General– *Security and protection.*

General Terms
Measurement, Experimentation, Security.

Keywords
Handover, IEEE 802.11i, WiFi, pre-authentication, re-authentication, IAPP.

1. INTRODUCTION
With the falling cost and power consumption of wireless LAN chipsets and software, wireless LAN are proliferating everywhere, and have emerged as a competitive technology to meet requirements users have on the Internet access availability, even in mobile environment. In this context the security is more difficult to provide in wireless environment than with legacy wired technologies. This is due to the nature of the wireless radio media. In order to prevent eavesdropping the data transmitted on the air could be ciphered. The IEEE 802.11 standard define the Wired Equivalent Privacy (WEP) mechanism, but the static nature of the cipher key and some design drawbacks in the authentication mechanism make this solution usually considered as non secure. In order to enhance the security of 802.11 wireless networks, IEEE has designed a security extension called IEEE 802.11i. It defines a complete mutual authentication mechanism based on EAP and 802.1x. It associates this mechanism to a key exchange algorithm that allows stations to use dynamic ciphering material. Unfortunately, the overall extension has an impact on networks and devices performances. It is not really important, that the station spent time during the first association, but, as the cipher key is a secret shared between the station and its AP, the station has to re-authenticate with the new AP in order to get a new cipher key each time it handoffs. Therefore the re-authentication mechanism needs to be very responsive. However, current handoff schemes cannot meet time requirements real-time multimedia applications have.

Fast handoff management procedures have been proposed and studied by many researchers [1, 2, 3, 5, 7, 8, 13, 16 18, 19, 20] in order to shorten at best the handoff latency time, yet for real-time multimedia service such as VoIP, the handoff latency still has to be reduced in order to satisfy the quality of service needed by such applications. More, few of these research works are dealing with secured Wireless LANs.
Wireless voice-over-IP applications require highly interactive response during mobility and are extremely sensitive to network outages and delays [17]. In fact, supporting voice and multimedia with continuous mobility implies that the total latency of handoffs between base stations must be adequately small. Specifically, the overall latency should not exceed 50 ms to prevent excessive jitter [12]. Moreover, the limited range of 802.11 radios makes handoff actions highly probable for continuously mobile clients, such as a user walking with an 802.11-based phone.

Typically, a handoff can be divided into three phases: detection, search and execution. The detection phase corresponds to the time needed by a station to discover that it is out of range of its current access point (AP). At this point the station launches the search phase where it looks for a potential new access point

listening all 802.11 frequencies. The execution phase corresponds to the re-association followed by the re-authentication with the new access point the station has just chosen.

Many previous works have studied and proposed fast handoff procedures. In [7], the authors aim to reduce the detection phase time. A station starts the search phase whenever the transmission of a frame and its two consecutive retransmissions fail, the station can conclude that the frame failure is caused by the station's movement (i.e., further handoff process (search phase) is required) rather than a collision. As described in [1], the scanning latency is the dominant latency component. To reduce this scanning latency, a new scheme was proposed in [16]. Such a scheme reduces the total number of scanned channels as well as the total time spent waiting on each channel. Specifically, two algorithms were introduced: NG (neighbor graph) algorithm and NG-pruning algorithm. The NG algorithm uses the neighbor graph whereas the NG-pruning algorithm further improves the channel discovery process by using a non-overlapping graph. In [18] and [19], the authors proposed a fast Inter-AP handoff scheme based on the predictive authentication method defined in IEEE 802.11i [10]. To predict the mobility pattern, the frequent handoff region (FHR) has been introduced. The FHR is formed by APs having the highest probabilities to be the next AP visited by a station upon handoff. A mobile station pre-authenticates according to the IEEE 802.1x [11] model with only APs within the FHR. Authors in [3] proposed a pre-authentication method based on proactive key distribution following the recent and predominant wireless network authentication method amended by the IEEE 802.11i security group [10] (the predictive authentication procedure). They introduced a data structure, called the Neighbor Graph, which dynamically captures the ever-changing topology of the network, and hence tracks the potential APs to which a station may handoff to in the near future.

The complete handoff latency in 802.11 networks with 802.11i security has been reduced to about 70 ms, which is still above the required 50 ms for proper operation of interactive real-time multimedia applications such as voice over IP. In fact, latency due to the detection and search phases has been reduced from around 500 ms to about 20 ms [1, 2, 5, 13, 8]. Fast re-authentication methods, based on the predictive authentication mechanism, reduce re-authentication from around 1.1s to about 50 ms [3]. However, it is rather interesting to note that neither the implementation nor the conducted measurements as reported in [3] do respect the exchanges specified in IEEE 802.11i and yet they do not take into account the load conditions of the network.

In this paper, we propose two new pre-authentication methods called: "Proactive Key Distribution (PKD) with anticipated 4-way-Handshake" and "PKD with IAPP caching". Our aim is to reduce the duration of the authentication exchange between the station and the network to its minimum while guarantying conformity with the IEEE 802.11i security standard. These two methods present a clear improvement over the pre-authentication method proposed in [3] at any given network load. We have measured the handover reduction on an actual test bed.

2. BACKGROUND

IEEE 802.1x provides a framework to authenticate and authorize devices connected to a network. It prohibits access to the network until such devices pass the authentication phase. The IEEE 802.1x standard provides a complete architecture that ensures the security through the concept of Controlled/Uncontrolled Ports at the link layer level. IEEE 802.1x has three main components: Supplicant, Authenticator and Authentication Server. It provides a framework to transmit key information between Authenticator and Supplicant [4].

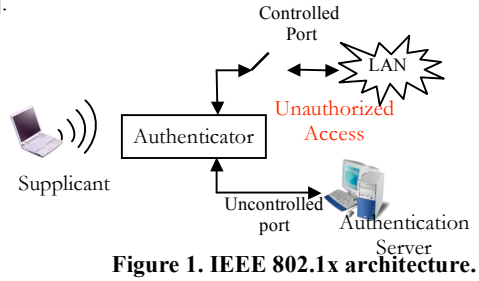

Figure 1. IEEE 802.1x architecture.

The IEEE 802.11i standard defines how to use the 802.1x in the context of IEEE 802.11 networks. For IEEE 802.11i, the access point (AP) takes the role of the Authenticator and the client (STA) the role of the Supplicant. The uncontrolled port is used to forward authentication traffic between the Supplicant (STA) and the Authentication Server (figure 1). Once the Authentication Server has successfully concluded the mutual authentication with the Supplicant, the Authentication Server informs the Authenticator about the status of the authentication. Then, it sends to the Authenticator the keying material it has established with the Supplicant through an EAPOL-key exchange [9]. At this point, the Supplicant and the Authenticator share the same established keying material. If all exchanges have been successful, the Authenticator allows traffic from the Supplicant to flow through the controlled port, giving the client a full access to the network.

The IEEE 802.11i EAPOL-key exchange uses a number of keys. Key hierarchies have been defined to divide up initial key material into useful keys. The two key hierarchies are: Pairwise key hierarchy and Group key hierarchy keys. The first one defines individual keys specific to one client in the cell associated to one AP and it is used for authentication and unicast transmission. The second hierarchy is necessary in order to cipher broadcasted data; therefore it has to be shared between an AP and all clients associated to it.

The starting point of the pairwise key hierarchy is the pairwise master key (PMK) generated separately by the Supplicant and the Authentication Server. They use the same pre-shared key exchanger during the mutual authentication. A pseudorandom function is run over the PMK and other parameters to create the pairwise transient key (PTK). The PTK gets divided into three keys. The first key is the EAPOL-key confirmation key (KCK). The KCK is used by the EAPOL-key exchanges to provide data authenticity. The second key is the EAPOL-key encryption key (KEK). The KEK is used by the EAPOL-key exchanges to provide confidentiality. The third key is the temporal key, which is used by the data-confidentiality protocols (TKIP or CCMP). The starting point of the group key hierarchy is the group master key (GMK). The GMK is a random number. A pseudorandom function gets run over the GMK and some other parameters to create the group temporal key (GTK) which is used to cipher broadcast traffic.

2.1 EAP/TLS Authentication Process

In an IEEE 802.11i exchange using EAP/TLS, the Supplicant and the Authentication Server start a mutual authentication through a secure tunnel. Authentication messages are exchanged between

the Supplicant and the Authentication Server through the access point (Authenticator) via the uncontrolled port. The following temporal diagram (figure 2) portrays the complete detailed sequence of messages exchanged between the different entities during a complete EAP-TLS authentication.

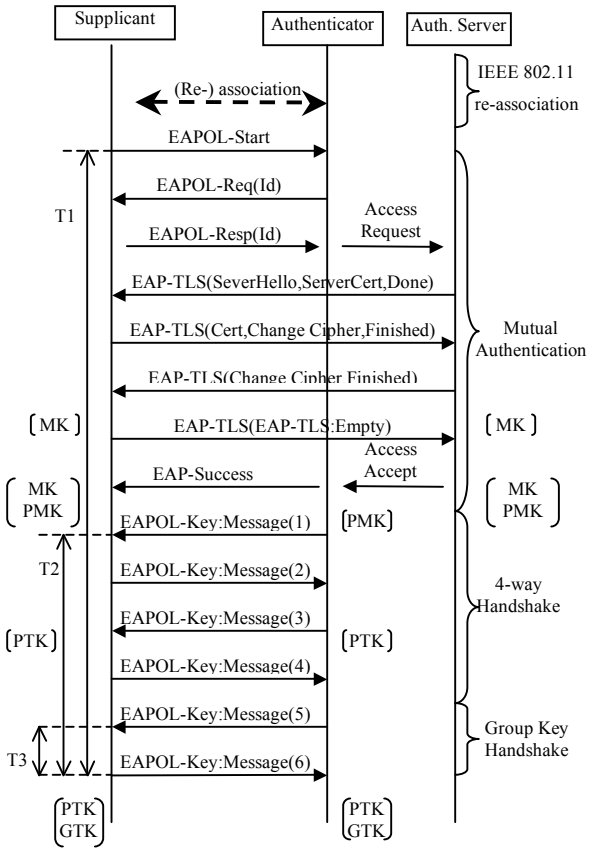

Figure 2. Complete Authentication exchange (with EAP/TLS).

The 4-way handshake does several things: confirms the PMK between the supplicant and the authenticator, establishes the temporal keys to be used by the data-confidentiality protocol, authenticates the security parameters that were negotiated and provides keying material to implement the group key handshake. The group key handshake, however, is needed each time a client handoffs to update the GTK with the one corresponding to the new AP.

3. PROACTIVE KEY DISTRIBUTION

The PKD (Proactive Key Distribution) method defines a proactive key distribution between a mobile station and access points. Thus, it establishes authentication keys before even the re-association. Upon handoff, authentication exchange between station and its access point is reduced to the 4-way-handshake and the Group Key Handshake phases. This method is based on an Accounting Server responsible to manage a Neighbor Graph for all network access points [3]. We will consider that the functionalities of authentication and accounting are gathered in a single AAA Server (Authentication, Authorization, and Accounting Server).

In contrast to IEEE 802.11i, PMK are derived through the following recursive equation:

$$PMK_0 = PRF(MK, \text{'client EAP Encryption'} \mid clientHello.random \mid ServerHello.random) \quad (1)$$

$$PMK_n = PRF(MK, PMKn\text{-}1 \mid APmac \mid STAmac)$$

The fist PMK key is derived from the master key and random sequences (generated by the server and the client) using the same method as in legacy 802.11i [10]. Then, PMK_n (where n represents the nth station re-association) is generated using: the PMK_{n-1} generated during the last association, the MAC address of the targeted AP and the MAC address of the station. The client and the AAA server know all these parameters and then every one can derive separately the PMK key.

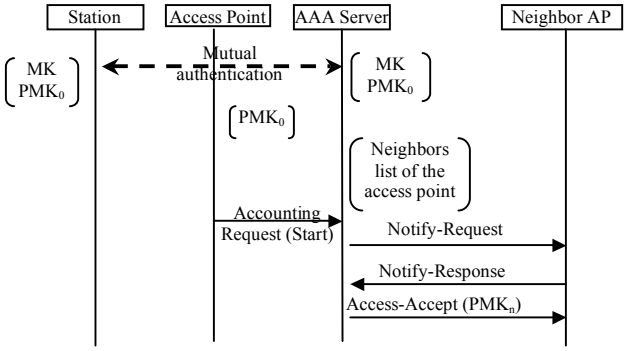

Figure 3. Pre-authentication exchange with PKD method.

After the first mutual authentication between the station and the AAA server, the access point sends to the AAA server an Accounting-Request (Start). Consequently, the AAA informs each access point in the neighborhood of the current access point of the station about a possible handoff of the station through a Notify-Request message. At this point, each neighbor access point responds to the AAA Server with a Notify-Response message that initiates generation of the PMK_n based on the equation (1). Then the AAA server sends the keys to the access point using an ACCESS-ACCEPT message [1]. Figure 3 portrays the exchange carried out with just one of the AP neighbors.

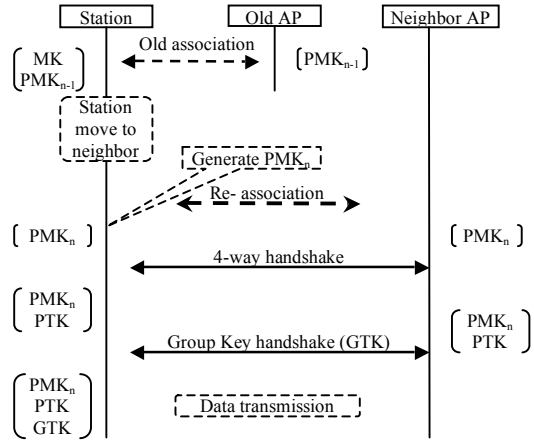

Figure 4. Re-authentication exchange with PKD.

Upon a handoff to a new access point the station gets the MAC address of the access point and then calculates a new PMK_n using the second part of the formula (1). This key is equal to the one already sent by the AAA server to the access point. All what is needed to check the liveness and the freshness of the

corresponding key hierarchies is to perform a 4-way handshake and a group key handshake as shown in figure 4.

4. PROPOSED METHODS

A full IEEE 802.11i exchange, as already portrayed on figure 2, requires 14 messages and last an authentication time denoted T1 and evaluated to 1.1s according to [3]. This time value further increases the handoff latency, and by itself represents an unacceptable value for multimedia and interactive applications. To decrease the authentication latency upon handoffs, previous works [19] and [3] restrict authentication phase exchange to the only messages exchanged between the station and the access point. They anticipate the mutual authentication exchange between the stations and the authentication server (i.e., pre-authentication).

Hence, the PKD method restricts the re-authentication exchange to the 4 Way Handshake and the Group key Handshake (a total of 6 messages) and consequently limits the time needed to complete the authentication to only T2 (see figure 2). This method was evaluated experimentally in [3] where measurements estimated T2 to 50 ms. While this result indicates a significant reduction in authentication time compared to a complete IEEE 802.11i (1.1 ms), the implementation described performs only two messages exchange between a station and the access point instead of the complete 4-way-handshake. They did not give any indication on the Group-Key-Handshake. Moreover, network conditions such as the actual network load are not taken into account. As a part of our testbed, we implemented the PKD method and indeed found that the re-association time depend on the network load, since each message need more time to be successfully transmitted as the load increases.

In this work, we aim to reduce the exchange between the station and its new access point to its minimum during the re-association. This is done by anticipating the 4 Way Handshake and restrict re-authentication to just the Group key Handshake (2 messages). This reduces the latency time to T3 as shown in figure 2. Two re-authentication methods implementing this principle are proposed, implemented and evaluated as stated in the following: “PKD with IAPP caching” and “PKD with anticipated 4-way Handshake”.

4.1 PKD With IAPP Caching

In this approach, we propose to combine PKD keys pre-distribution with the use of the cache mechanism defined in the Inter Access Point Protocol (IAPP), which is a part of the IEEE 802.11f standard.

IAPP protocol [9] is a mechanism that allows the transfer of the context related to a mobile station from the previous access point to the new one upon handoffs. More, it defines a cache mechanism that allows access points to exchange this information pro-actively, i.e. before re-association. The cache management is based on a neighbor graph maintained by each access point. This graph contains the list of AP neighbors to whom an access point must relay the contexts of its associated stations. Upon a station association, the access point transfers the station context to its AP neighbors using a CACHE-notify message. Each neighbor answers with a CACHE-response message in order to confirm its cache has been updated. To secure IAPP exchanges between access points, IEEE 802.11f uses the RADIUS protocol. In fact, RADIUS provides access point’s mutual authentications and ensures the confidentiality of the context transfers over the distribution system [9].

In addition to PMKs pre-distribution defined in the PKD method, we use IAPP context transfer in order to perform a pre-distribution of PTK keys. The station will use these keys to temporarily re-associate with a new access point avoiding the 4-ways Handshake. Only a simple Group-Key-Handshake remains necessary. Pre-distributed PTKs are calculated by the current access point and sent to the neighbors APs. The key corresponding to neighbor AP_X is calculated with the following equation:

$$PTK_X = PRF\ (PMK, PTK_{init} \mid STAmac \mid AP_X\ mac) \qquad (2)$$

Where STAmac and AP_Xmac are respectively the address MAC of the station and the AP_X.

A mobile station will be able to calculate the key corresponding to its new access point as soon as it knows its MAC address. A PTK allows it to be authenticated with this access point through a Group-Key-Handshake. This is a temporary authentication. Indeed, the station engages immediately a legacy PKD authentication with its new access point while continuing its data transmission. We define TIMER_AUTH to be the time limit within which the station must have performed a complete authentication.

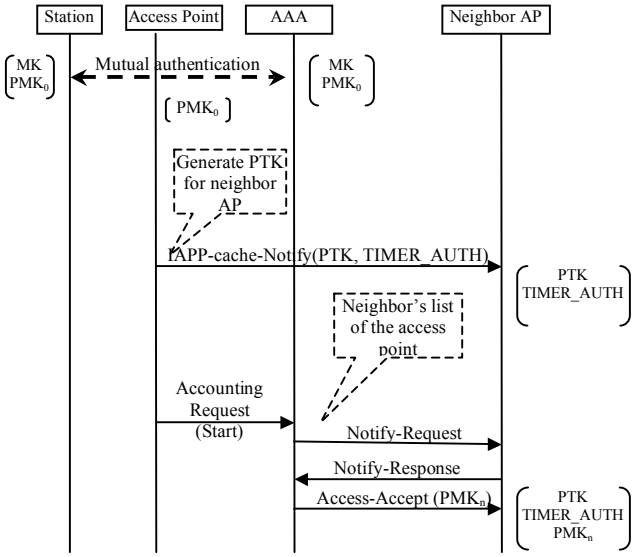

Figure 5. Pre-authentication exchange with « PKD with IAPP caching » method.

The different steps of the method are described below:

- Upon a station re-authentication, the access point consults its neighbor graph and starts IAPP exchange to update neighbor’s caches. The station context transferred by the access point contains: a PTK key and the TIMER_AUTH value,
- The current access point informs the AAA server about this station association in order to start the PMKs generation used to complete the predictive authentication procedure.

Figure 5 shows messages implied in these two exchanges with a given neighbor access point.

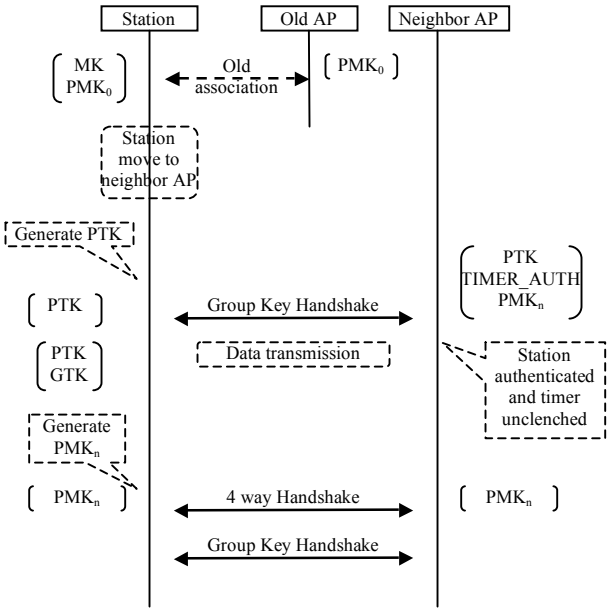

Figure 6. Re-authentication exchange with « PKD with IAPP caching » method.

- As shown in figure 6, when the station moves to a neighbor access point, it starts Group-Key-Handshake using the PTK computed using the formula 2. After what it is able to transmit data. Then, the access point starts a timer while waiting for a 4-way Handshake with PMK_n. The value of this timer has do not exceed the $TIMER_AUTH_{sta}$.
- During the data transmissions, and before timer expiration, station starts 4-way Handshake in order to calculate a new permanent PTK.

The new access point will start the PTK keys distribution to AP neighbors only after the station authentication has been completed.

4.2 PKD With Anticipated 4-way Handshake

We propose here an improvement that does not affect the Proactive Key Distribution method and does not involve any protocol between APs. The main idea is to anticipate the 4-way-Handshake exchanges between a station and AP neighbors through the current access point which is reachable on the LAN trough the distribution system. Once again, this improvement enables us to restrict the re-authentication to the only Group-Key-Handshake (2 messages) exchange. As for the previous method, this will also reduce the re-authentication time to its minimum (within the IEEE 802.11i mechanism).

The AAA server sends to the station a list of neighbor access points that have answered the Notify-Request in the PKD exchange (cf. 4.1). Upon a station association or re-association, its access point informs the AAA server in order to start proactive keys distribution. All neighbors APs will receive PMK keys related to the station. The station also receives a neighbor's list (List_AP) containing the list of AP neighbors of the current AP. The station will have to carry out a pre-authentication through the distribution system (via its current access point) with these APs. As shown in figure 7, the station carries out a 4-way-Handshake with a neighbor access point through its current access point with a PMK_n key calculated by equation (1) thanks to the MAC address of the neighbor AP learned from the list_AP.

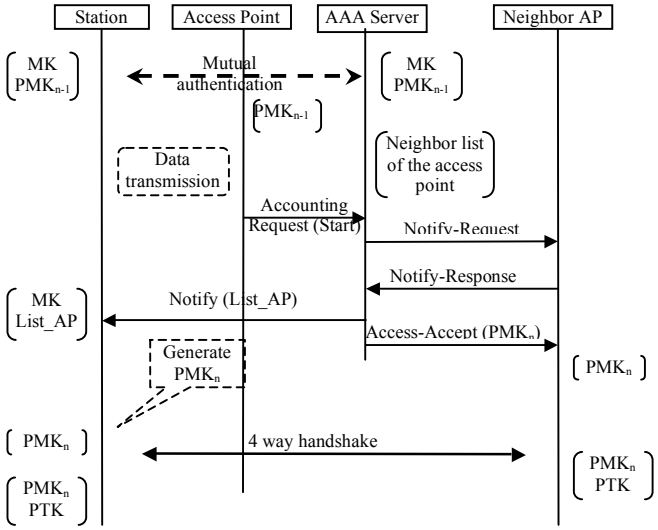

Figure 7. Pre-authentication exchange with « PKD with anticipated 4-way Handshake » method

When the station moves towards a neighbor access point two cases could happen:

- The station has already calculated the PTK through the pre-authentication and thus it only carries out a Group-Key-Handshake to complete the authentication;
- The station has not yet completed the pre-authentication, and thus it carries out a 4-Way-Handshake and a Group Key Handshake corresponding to the full PKD method.

The only difference in the first case is that the station performs the 4-way Handshake before the handoff rather than after.

4.3 Conclusion

«PKD with IAPP caching" and "PKD with anticipated 4-way Handshake" both restrict the re-authentication exchange to two messages known as the Group Key Handshake. They both reduce the re-authentication time to T3 and then offer the same performance in term of handoff latency. However the two methods operate in very different ways.

In the "PKD with anticipated 4-way Handshake" method, PTK generation (figure 7) is anticipated via the current access point. The traffic generated by these exchanges depends on the number of AP neighbors and on the handoff frequency. Indeed for each new association, a station carries out the pre-authentication exchanges with the neighbor access points using the wireless transmission. This is done in parallel with the data transmission and authentication traffic share the same resources as the application data. If it is not without consequences on the traffic, the amount of traffic generated by authentications is quite limited. This method also supposes to transmit the list of AP neighbors in the Notification message.

On the other hand in the "PKD with IAPP caching" method, current access point distributes PTKs keys using the IAPP context transfer functionality. As shown in figure 5, this exchange is carried out through the distribution system and therefore has no influence on the wireless LAN load, which is scarce by nature.

There is also a concern, since in IEEE 802.11i an access point is not supposed to know the PTK used by another access point. Or, in this method the previous access point know the PTK temporally used by the current access point. But as this PTK is used only during a short time between the first Group Key Handshake and the 4-way Handshake (less than TIMER_AUTH), the security is not really compromised.

Many IEEE 802.11 products manufacturers did not adopt the IAPP protocol, and then it is extremely probable that hotspot access points for example, will not be able to support "PKD with IAPP caching" method. That is why it is useful to offer an alternate pre-authentication method that allows the same re-authentication performances.

5. IMPLEMENTATION AND PERFORMANCE EVALUATION

5.1 Test-bed Set Up

In a previous work, we described an IAPP implementation integrating a context transfer protocole between IEEE 802.11 access points [15]. This implementation is based on Hostap software [14]. We have enhanced our test-bed with the support of secure fast handoff by integrating the PKD method as well as our two improvements “PKD with anticipated 4-way Handshake“ and ”PKD with IAPP caching". In our testbed we use EAP/TLS and RADIUS server respectively as authentication method and authentication server. For supplicant implementation we have chosen the wpa_supplicant software that is a component of the Hostap project. FreeRadius [6] is used for the RADIUS server. We modified this software in order to deal with Accounting Server functionalities (neighbors graph handling and the key pre-distribution). Authenticators are access point software based on the Hostap to which we have added IAPP protocol. Hostap and wpa_supplicant allow setting up an IEEE 802.11i authentication [14]. We modified these two softwares in order to support the pre-authentication. We have also modified Hostap software to be able to communicate with Accounting Server at the key pre-distribution phase.

With these modifications, our test-bed now allows all the three pre-authentication methods we have described. Thus a mobile station can negotiate with the access point which pre-authentication method is to be used. This negotiation will take into account station capabilities and also IAPP activation among access points.

5.2 Handover Time Evaluation

We have set up this test-bed in order to evaluate handover effects on the traffic exchanged by mobile stations under different network conditions. We have also studied the influence of the load condition to the re-association process.

First, we have evaluated the re authentication time for each of the three methods:

- Proactive Key Distribution (PKD);
- PKD with IAPP caching;
- PKD with anticipated 4-ways handshake.

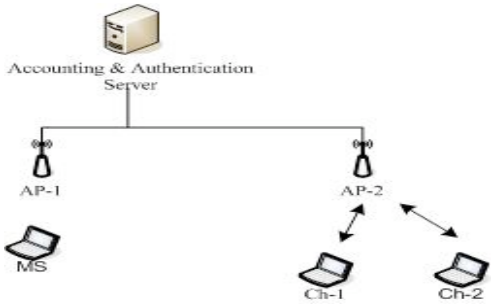

Figure 8. Measurement test-bed.

We considered two access points and a mobile station (MS). This station performs handovers from AP-1 to AP-2. The re-authentication time is measured analyzing the AP-2 logs. In order to evaluate the re-authentication time as a function of the network load, we added two stations STA-1 and STA-2 both associated with AP-2. Both these station generate traffic within the AP-2’s cell. The traffic is generated, using the D-ITG [21] tool, it produces an UDP traffic with a 500 Kb packet size with an inter-packet time distributed exponentially.

The measurements have been done under a fixed data rate equal to 2 Mb/s, which is equal to the IEEE 802.11 basic rate. This is needed to prevent stations to arbitrary use different uncontrolled data rates varying between 11 Mb/s and 2Mb/s according to the quality of the signal or the number of retransmission. This could vary dynamically from station to station and from time to time.

The figure 9 portrays the re-authentication latency as a function of the traffic load of the AP2’s cell. This traffic load is the sum of the traffic generated by the stations STA-1 and STA-2. There are two curves in this figure: the first one represent the evolution of re-authentication latency for the PKD methods and the second one for the two improvements we have proposed.

For the PKD method, the re-authentication time represents the time separating the sending of the first message of the 4-way Handshake (AP-2 → MS) and the reception of the last Group Key Handshake message (MS → AP-2). For both PKD with IAPP caching and PKD with anticipated 4-way Handshake, the re-authentication time represents the time between the sending of the first Group Key Handshake message and the reception of the second message.

We clearly observe that the re-authentication time experienced by the PKD method varies as a function of the traffic load and does not correspond to the results presented in [3]. PKD requires a re-authentication latency varying from about 70 ms under very light load condition, and increases up to hundreds of ms at heavy loads. We recall that the authors in [3] stipulate a latency of about only 50 ms. The difference may come from limitations and assumptions they used in this work. In contrast, the two methods we have proposed require a re-authentication latency lower than the 50 ms limit even at high loads. Hence, they represent a clear improvement over the PKD method.

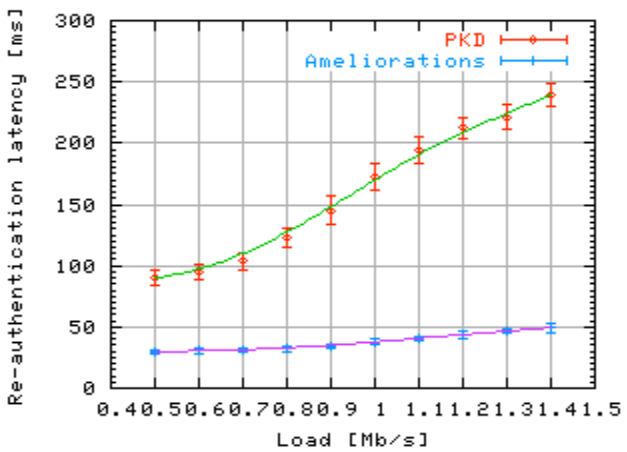

Figure 9. PKD and ameliorations re-authentication time.

Recall from figure 2 that the re-authentication phase is started only once the re-association phase has been completed. At very high loads, the AP may not authorize fast enough new re-associations. Then the overall re-association process fails. A question arises: "How much traffic could the AP sustain while operating properly new associations and re-associations. Figure 10 represents the time spent at the AP to fulfill a new association, denoted by the association latency, as a function the submitted load.

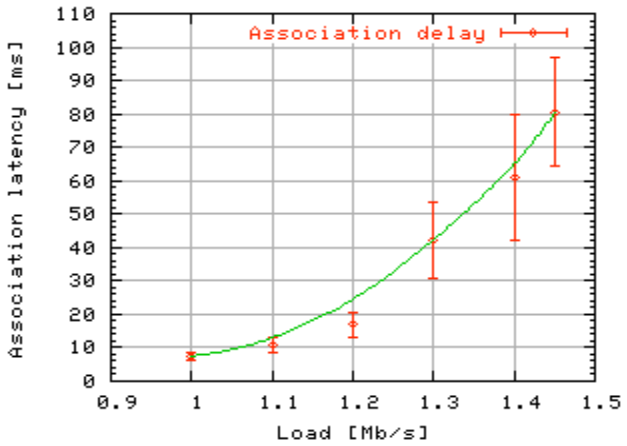

Figure 10 . Re-association time evolution.

We could see that this time increases rapidly as a function of the load in the AP2's cell. Beyond a load of about 1.45 MB/s, the station is no more able to join the access point. A detailed analysis of the actual exchanges done between MS and AP-2 showed that after a certain delay the station ignores any eventual Authentication/Association Response messages and reinitiates the overall association phase. We conjecture that this delay is aimed to prevent a station from joining an already congested access point and to reduce the number of station managed by an overloaded access point. We can deduce from the figure 10 a timer of about 80 ms.

6. CONCLUSION

In this paper, we proposed new re-authentication methods: "PKD with IAPP caching" and "PKD with anticipated 4-way Handshake". These two methods present a clear improvement over the PKD method suggested in [3] at all realistic network loads. A test-bed has been developed that supports secure fast handoffs integrating the PKD method as well as our proposed methods. Experiments performed over this test-bed proved the interest of our methods. Re-authentication latency has been reduced under the target limit (50 ms) even under high load conditions. This allows real time applications to work on a secure IEEE 802.11 networks. More measurements are underway to further evaluate the proposed methods specially scalability issues.

In future works, we plan to explore intra technologies handovers and then to extend our methods to support pre-authentication between heterogeneous networks like IEEE 802.11 and IEEE 802.16.

7. REFERENCES

[1] A. Mishra, M. Shin and W. Arbaugh: An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process. ACM SIGCOMM Computer Communications Review, Vol. 33, No. 2 ,April 2003.

[2] A. Mishra M. Shin and W. Arbaugh.: Context Caching using Neighbor Graphs for Fast Handoffs in a Wireless Network. IEEE INFOCOM conference, Hong Kong ,March 2004.

[3] A. Mishra, M. Shin and W. Arbaugh. : Pro-active Key Distribution using Neighbor Graphs. IEEE Wireless Communications, vol. 11,February 2004.

[4] Blunk Larry and John Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", IETF RFC 2284, March 1998.

[5] C. L. Tan et al.: A fast handoff scheme for wireless network. Proc of the 2 nd ACM Intl Workshop on Wireless Mobile Multimedia, Seattle, August 1999.

[6] FreeRadius: The FreeRadius Server Project. URL: http://www.freeradius.org,March 2005.

[7] H. Velayos and G. Karlsson, "Techniques to Reduce IEEE 802.11b MAC Layer Handover Time" Proc. IEEE ICC, June 2004.

[8] Hye-Soo Kim, Sang-Hee Park, Chun-Su Park and al. .: Selective Channel Scanning for Fast Handoff in Wireless LAN using NeighborGraph. The 2004 International Technical Conference on Circuits/Systems Computers and Communications (ITC-CSCC2004) Japan, July 2004.

[9] IEEE 802.11f: IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation. IEEE, July 2003.

[10] IEEE 802.11i: Amendment 6: Medium Access Control (MAC) Security Enhancements. IEEE Computer Society, April 2004.

[11] IEEE 802.1x: IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control. IEEE, June 2001.

[12] International Telecommunication Union: General Characteristics of International Telephone Connections and International Telephone Circuits. ITU-TG.114, 1988.

[13] Ishwar Ramani and al.: SyncScan: Practical Fast Handoff for 802.11 Infrastructure Networks. Proceedings of the IEEE INFOCOM Conference, Miami, March 2005.

[14] Jouni Malinen: Host AP driver for Intersil Prism.URL:http://hostap.epitest.fi/, March 2005.

[15] M.Kassab, A.Belghith, J.M.Bonnin and H.Idoudi: Réalisation d'un point d'accès logiciel 802.11b .SETIT 2004, Tunisia, March 2004.

[16] M. Shin, A. Mishra, and W. Arbaugh: Improving the Latency of 802.11 Hand-offs using Neighbor Graphs. Proc. ACM Mobisys, September 2004.

[17] T. Henriksson: Hardware architecture for 802.11b based h.323 voice and image ip telephony terminal. Swedish system-onchip conference2001, Proceedings of the SSoCC, Sweden ,March 2001.

[18] . Sangheon Pack and Yanghee Choi: Fast Inter-AP Handoff using Predictive-Authentication Scheme in a Public Wireless LAN. IEEE Networks, August 2002.

[19] Sangheon Pack and Yanghee Choi: Pre-Authenticated Fast Handoff in a Public Wireless LAN based on IEEE 802.1x Model. IFIP TC6 Personal Wireless Communications, October 2002.

[20] S. Pack, H. Jung, T. Kwon and al..: SNC: A Selective Neighbor Caching Scheme for Fast Handoff in IEEE 802.11 Wireless Networks. ACM SIGMOBILE Mobile Computing and Communications Review, February 2004.

[21] Stefano Avallone and al.: D-ITG, Distributed Internet Traffic Generator. URL: http://www.grid.unina.it/software/ITG/ , May 2005