Fast and secure handoffs 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, ENSI, Tunisia
{Mohamed.kassab,Abdelfattah.belghith,
sahbi.sassi}@ensi.rnu.tn
[2] Ecole Nationale Supérieure de Télécommunications de Bretagne, ENSTB, France
Jmb.bonnin@enst-bretagne.fr

Abstract. User mobility in IEEE 802.11 wireless LANs is ever increasing due to wireless technological advances, the recent popularity of portable devices and the desire for voice and multimedia applications. These applications, however, require very fast and secure handoffs among base stations to maintain the quality of the connections. Re-authentication during handoff procedures causes a long handoff latency which affects the fluidity and service quality of interactive real-time multimedia applications such as VoIP. Minimizing the re-authentication latency is crucial in order to support real-time multimedia applications on public wireless IP network. In this paper, we propose two fast re-authentication methods based on the predictive authentication mechanism defined by IEEE 802.11i security group. We compare our proposed methods to already existing ones. We have implemented these methods in an experimental test-bed using freeware and commodity 802.11 hardware. Conducted measurements show significant latency reductions compared to other proposed solutions.

1 Introduction

With the ever falling cost and power consumption wireless LAN chipsets and software, wireless public LAN systems based on IEEE 802.11 are becoming popular in hot spot areas. Public wireless LAN systems provide a high-speed Internet connectivity of up to 11Mbit/s, yet they should support different user mobility patterns. User authentication and handoff support between access points (APs) are therefore among the most important issues to be considered in the design of public wireless LAN systems. Generally, since a mobile station need to be authenticated during and after a handoff, a mobile station upon a handoff should perform a new authentication procedure and receive new data encryption keys. This authentication procedure requires the exchange of more than a dozen of messages and therefore impacts on the network performance. What is required is both a fast handoff technique coupled with a fast predictive authentication procedure.

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 minimize the handoff latency

Please use the following format when citing this chapter:

Kassab, M., Belghith, A., Bonnin, J.-M. and Sassi, S., 2007, in IFIP International Federation for Information Processing, Volume 229, Network Control and Engineering for QoS, Security, and Mobility, IV, ed. Gaïti, D., (Boston: Springer), pp. 61–74.

time, yet for real-time multimedia service such as VoIP, the problem of handoff latency still has to be shortened in order to satisfy the quality of service needed by such applications. Supporting voice and multimedia with continuous mobility implies that the total latency of a handoff must be adequately small [17]. Specifically, the overall latency should not exceed 50 ms to prevent excessive jitter [12].

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 itself being out of range of its access point. At this point, the station launches the search phase for potential new access points. The execution phase corresponds to messages exchange allowing the station to re-associate and re-authenticate with the new chosen AP. 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 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) was introduced. The FHR is formed by APs having the highest probabilities to be next visited by a station upon handoff. A mobile station pre-authenticates according to the IEEE 802.1x [11] model with only APs given by 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 IEEE 802.11i authenticated handoff latency is brought to about 70 ms, a latency still above the required 50 ms target for the proper operation of interactive real-time multimedia applications such as voice. 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 authentication exchanges between the station and the network to its minimum while guarantying conformity with the IEEE 802.11i security proposal. These two methods present a clear improvement over the method of pre-authentication suggested in [3] at any given network load. We show these improvements via measurements conducted on an actual test bed.

2 Background

2.1 The 802.11i standard

The IEEE 802.11i standard specifies the use of the IEEE 802.1X protocol [11] which offers a general framework to build an authentication service and keys distribution. This protocol uses EAP (Extensible Authentication Protocol) layer, standardized by the IETF (Internet Engineering Task Force), for the support of authentication methods [4]. One of the methods which correspond to the specification of IEEE 802.11i is EAP/TLS [10].

The IEEE 802.1X standard provides an architectural structure, basing on the «Controlled/Uncontrolled Port " concept, for controlling access to the network on link layer. It provides a skeleton of security by defining three entities: Supplicant, Authenticator and the Authentication Server. A client is an entity who wishes to use a service (MAC connectivity) offered via the controlled port. This client authenticates himself to an Authentication Server through authenticator. In case of success, the server orders authenticator to allow the service.

IEEE 802.1X uses Extensible Authentication Protocol (EAP) to define how messages are exchanged between network entities: Supplicant, Authenticator and Authentication Server. EAP has defined a standard exchange of messages between entities using an agreed authentication protocol. The most known authentication protocols supported by EAP are: EAP-MD5 (Message Digest 5), EAP-TTLS and in our case the EAP-TLS (Transport Security Level). Figure 1 portrays the authentication protocols stack.

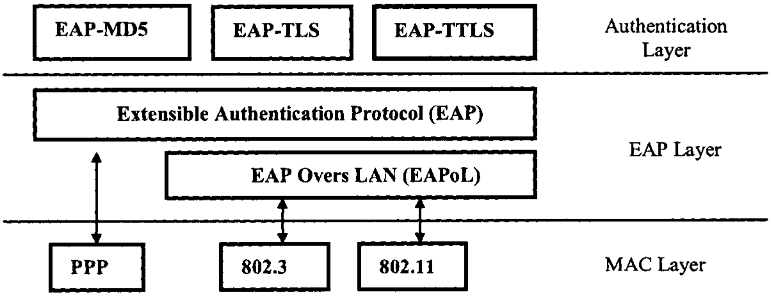

Fig. 1. Authentication Protocols

EAP does not specify the routing of the messages [4]. That's why, EAP messages must be encapsulated during their transfers. Thus, IEEE 802.1X defines the EAP over LAN (EAPoL) protocol to encapsulate the messages between Supplicant and Authenticator. The Authenticator relays authentication packets between

Authentication Server and Supplicant. In fact, Authenticator extracts EAP packets from IEEE 802.11 MPDUs and transmits them to Authentication Server.

In an IEEE 802.11i exchange using EAP/TLS, supplicant and Authentication Server start a mutual authentication. Authentication messages are exchanged between suppliant and Authentication Server over the access point (Authenticator) through the uncontrolled port.

Supplicant and Authentication Server generate separately a key named Master Key (MK). A second key is derived from the latter: Pairwise Master Key (PMK). Authentication Server sends this new key to the access point (Authenticator). Thus, the supplicant and the access point prove the possession of the same PMK, through an exchange of EAPOL-Key messages. This exchange is called the 4-Way-Handshake.

A second class of keys, « Group Transient Key » (GTK), is also defined for the broadcast traffic. Every Authenticator generates its own key and distributes it to associated stations.

4-Way-Handshake is an exchange of four EAPOL-Key packets between access point and Supplicant. It is initiated by the access point to:

- Prove that the pair has same key PMK.
- Derive a new key: Pairwise Transient Key (PTK) from the PMK.
- Install at the pair encryption key and control of integrity key.

GTK is sent by authenticator to the supplicant through the Group-Key-Handshake exchange who is composed of two EAPOL-Key messages.

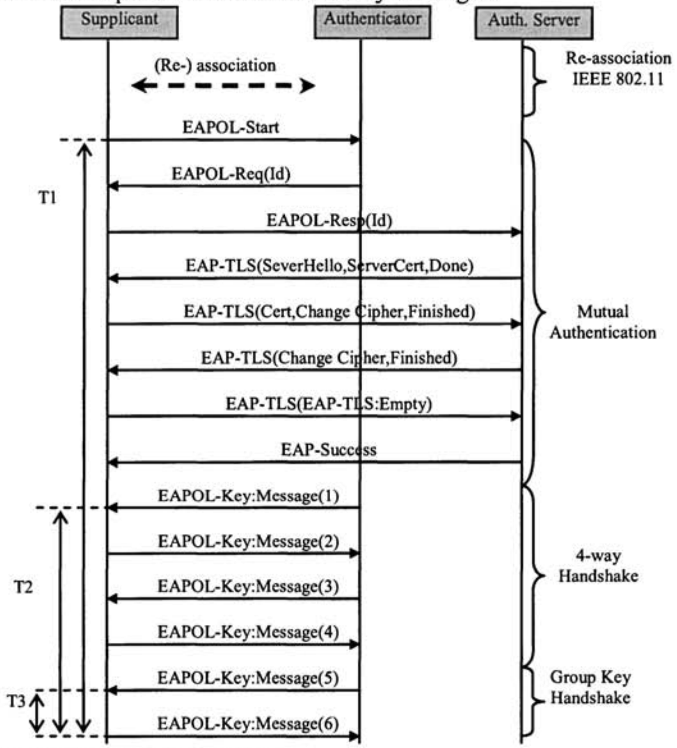

Fig. 2. EAP/TLS Authentication exchange

2.2 The Proactive Key Distribution

The PKD (Proactive Key Distribution) method defines a proactive key distribution between a mobile station and access points and thus establishes authentication keys before even the re-association. Upon handoff, authentication exchange between station and access point is reduced to 4-way-handshake and Group Key Handshake during the re-association. 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 will be 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:

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

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

Where n represents the n^{th} station re-association.

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

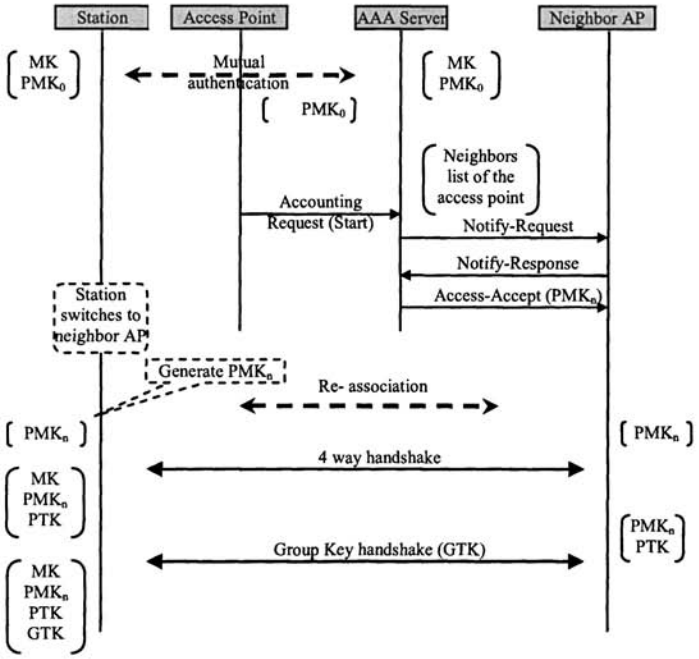

Fig. 3. Pre-authentication exchange with PKD method

Upon a handoff to a new access point, the station calculates a new PMK_n that is based on the generation parameters used and which corresponds to the key already sent by the AAA to the access point. All what is needed to check for liveness and freshness of the corresponding keys, is to perform a 4 way handshake and a group key handshake as shown in figure 4 below.

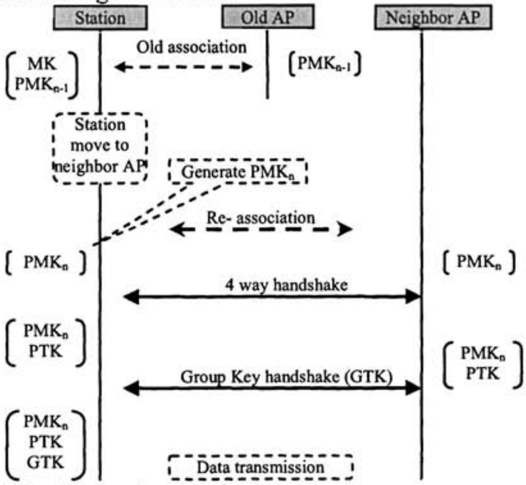

Fig. 4. Re-authentication exchange with PKD

3 Enhanced Pre-authentication Methods

A full IEEE 802.11i exchange, as already portrayed on figure 2 above, requires 14 messages requiring 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 only the messages exchanged between the station and the access point and anticipate exchange between station and authentication server (i.e., pre-authentication).

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 authentication time 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 as compared to a complete IEEE 802.11i (1.1 ms), their implementation performs only two messages exchange between station and access point instead of the complete 4-way-handshake and doesn't give any indication on Group-Key-Handshake. Moreover, network conditions such as the actual network load are not taken into account. As a part of our tested, we implemented the PKD method and indeed found different results as a function of the network load.

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

3.1 PKD with IAPP caching

In this approach, we propose to combine PKD keys pre-distribution with the use of the cache mechanism of the Inter Access Point Protocol (IAPP).

IAPP protocol [9] is a mechanism allowing to transfer mobile station contexts between access points. It defines a cache mechanism which allows access points to exchange information about moving stations before re-association. Cache management is based on a neighbor graph maintained at every access point. This graph contains the list of AP neighbors to which the access point must relay the contexts of its associated stations. Upon a station association, the access point transfers the station context to its neighbors through a CACHE-notify message. Each neighbor answers by a CACHE-response message in order to confirm his cache update. To secure IAPP exchanges between access points, IEEE 802.11f define the use of the RADIUS protocol. In fact, RADIUS ensures access point's authentication and context confidentiality through exchanges on the distribution system [9].

In addition to PMKs pre-distribution defined in the PKD method, IAPP allows PTKs keys pre-distribution. These keys will be used by the station to temporarily re associate with a new access point through a simple Group-Key-Handshake. Pre-distributed PTKs are calculated by the current access point. The key corresponding to neighbor X is calculated by the following equation:

$$PTK_X\text{=PRF (PMK, PTKinit |STAmac|APmac)} \qquad (2)$$

A mobile station will be able to calculate the key corresponding to its new access point. 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 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 perform a complete authentication.

Steps of the method are defined below:

- Upon a station authentication, the access point consults its neighbor graph and starts IAPP exchange to update neighbor's cache. 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 by these two exchanges with a given neighbor access point.

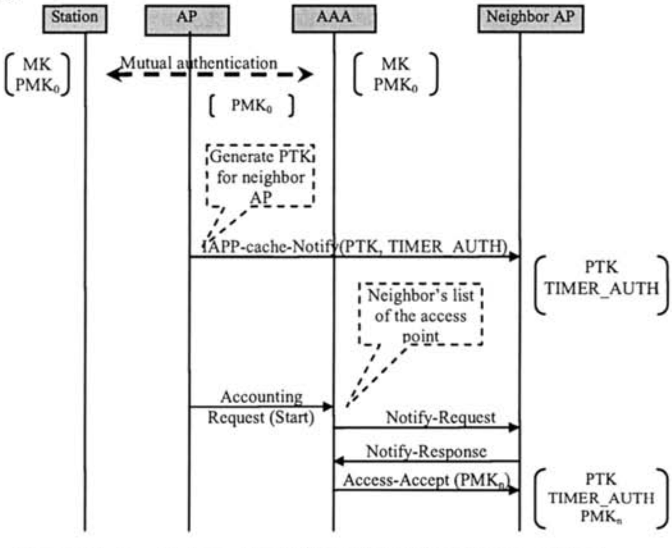

Fig. 5. Pre-authentication exchange with « PKD with IAPP caching » method

Let's take an example of an ESS with 3 neighbor access point A, B and C. The access point A send keys and timer corresponding to a station associated with it to neighbors B and C through IAPP messages. Access point B, for example, add PTK_B key and TIMER_AUTH timer to its IAPP cache and will use it in a future station re-authentication.

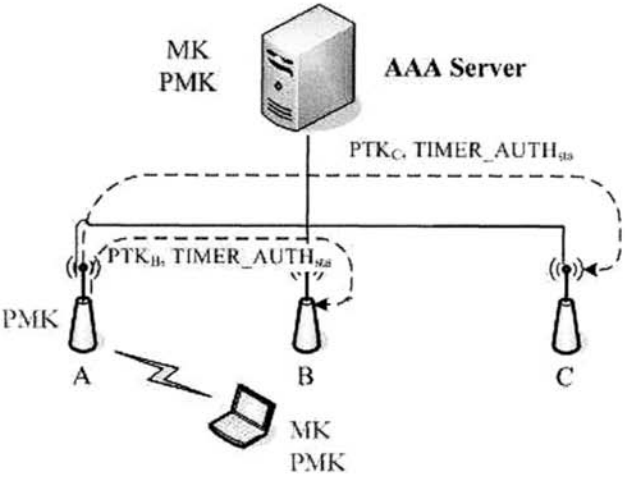

Fig. 6. Distribution of PTKs Keys with IAPP exchanges

- As shown in figure 7 below, when the station moves to a neighbor access point, it starts Group-Key-Handshake using the PTK and will then be 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 will not have to exceed the $TIMER\_AUTH_{sta}$
- Throughout data transmissions, and before timer expiration, station starts 4-way Handshake in order to calculate a new permanent PTK.

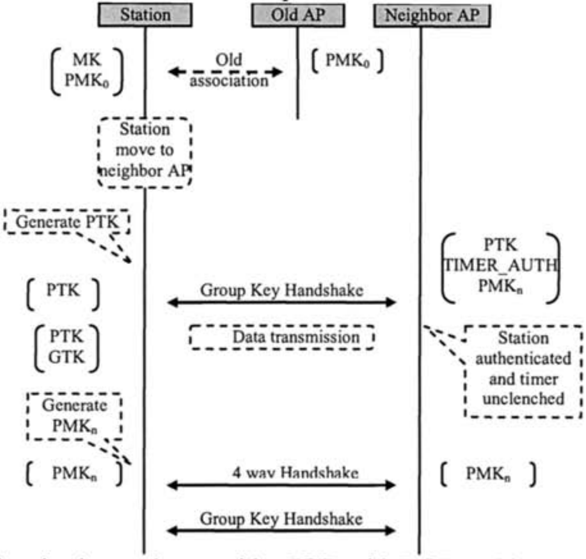

Fig. 7. Re-authentication exchange with « PKD with IAPP caching » method

3.2 PKD with anticipated 4-way Handshake

We propose here an improvement which does not affect the Proactive Key Distribution method. The main idea is to anticipate the 4-way-Handshake exchanges between a station and AP neighbors through the current access point. This improvement enables to restrict the re-authentication to the Group-Key-Handshake (2 messages) exchange, which enables us to reduce authentication time to its minimum (within the IEEE 802.11i mechanism). The AAA server sends to the station a list of neighbor access points which answered the Notify-Request in the PKD exchange (cf. 4.1).Upon a station association, its access point informs the AAA server in order to start proactive keys distribution. All AP neighbors will receive PMK keys corresponding to the associated station. Moreover, the station receives a neighbor's list (List_AP) with which it will have to carry out a pre-authentication through the distribution system (via its current access point). As shown in figure 8 below, 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).

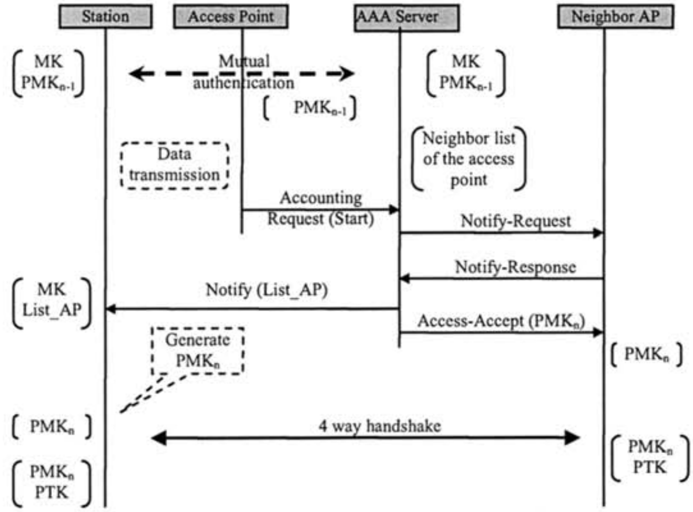

Fig. 8. Pre-authentication exchange with « PKD with anticipated 4-way Handshake » method

In the Figure 9 below, when a mobile station enter to the network and associate and authenticate itself to access point A, it will receive the neighbors AP list (B and C) from the AAA server. In other hand access point B and C, will receive keys corresponding to the mobile station (PMK^{B}_{n} and PMK^{C}_{n}). The mobile station would start a 4-way Handshake with access point B and C. The mobile station generate separately the PMK^{B}_{n} and carry out a 4-way Handshake with access point B in order to establish a PTK key that will be used, even the station move to B to start a Group-Key-Handshake.

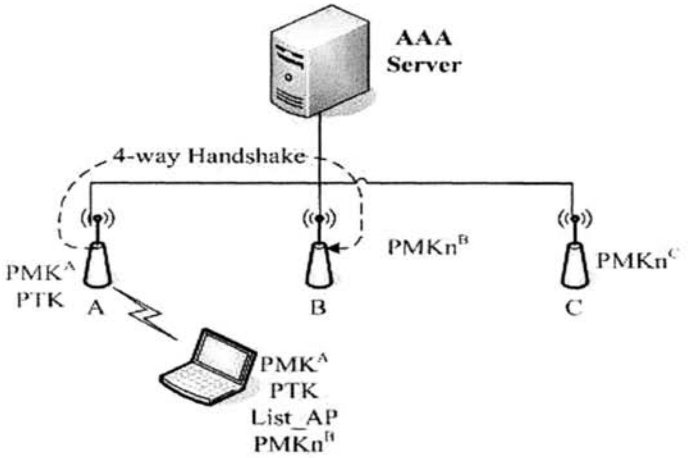

Fig. 9. Anticipation of the 4-way Handshake through the DS

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

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

4 Implementation and performance evaluation

In a previous work, we described an IAPP implementation integrating a context transfer through 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 handoffs by integrating the PKD method as well as our two improvements «PKD with 4-way anticipated Handshake» and «PKD with IAPP caching ". We use EAP/TLS and RADIUS server respectively as an authentication method and authentication server.

FreeRadius [6] was used to install RADIUS server. We modified this software in order to deal with Accounting Server functionalities (neighbors graph handling and the key pre-distribution). Authenticators are software access points based on the Hostap to which IAPP protocol was added. Hostap and wpa_supplicant allow setting up an IEEE 802.11i authentication [14]

We have evaluated the re authentication time for each one of the three methods and a full EAP/TLS authentication, in order to show the contribution of our two improvements " PKD with IAPP caching " and " PKD with anticipated 4-way Handshake ".

We considered two access points and a mobile station (MS). This station carries out handovers from AP-1 to AP-2. The re-authentication time is measured based on

AP-2 logs. These measurements were taken for EAP/TLS authentication, PKD methods and finally the proposed improvements. The latency measurements are given in the following table:

Table 1. Re authentication time in an empty network

	EAP/TLS Authentication	PKD	Proposed methods
Average	1,52532562	0,07344857	0,016413484
Variance	0,08018446	0,00022073	2,87917E-05

We remark that the latency induced by the PKD method is around 73 ms which exceeds the value of 50 ms as indicated by [9]. We note also that our improvements reduce latency time down to 16 ms, hence gaining 55 ms as compared to the PKD method.

5 Qualitative Comparison

The two enhancements proposed in this work restrict the re-authentication exchange to just the Group Key Handshake and they present the same performance in terms of handoff latency. However, they operate in very different ways during the pre authentication phase.

Firstly, the "PKD with anticipated 4-way Handshake" method anticipates the PTK generation (figure 7) via the current access point. The traffic generated for this PTK generation depends on the number of AP neighbours and on the actual handoff frequency. On the other hand in the "PKD with IAPP caching" method, the current access point distributes PTKs keys using the IAPP context transfer functionality using the distributed system infrastructure, hence not affecting the wireless media. Consequently, the two methods will be affected differently as a function of the network load. Moreover, under a high workload, using the "PKD with anticipated 4-way Handshake" method, a station may not be able to complete properly the pre authentication exchange and establish the needed keys. With the "PKD with IAPP caching", the cell load does not interfere with keys establishment (exchanged through the distribution system).

Secondly, the handoff frequency can also influence differently the performance of the two methods. In fact, with PKD with anticipated 4-way Handshake" a station must generate separately pre authentication keys for each neighbour AP and therefore the time needed for pre authentication is longer than for the "PKD with IAPP caching" where the keys are distributed by current access point. Consequently, for a fast moving station switching quickly between neighbours APs, it is most probable to have a key miss with the first method.

Thirdly, there may be a certain security concern with the "PKD with IAPP caching" since in the IEEE 802.11i, an AP is not supposed to know PTKs used by another APs.

But assuming confidence for the current AP and since such PTKs are only used 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.

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 feasible network load. A test-bed is developed that supports secure fast handoffs integrating the PKD method as well as our proposed methods. Experiments conduced over this test-bed proved the clear superiority of our methods. Re-authentication latency is then reduced down to approximately 16 ms, a value much under the targeted 50 ms and achievement that makes it possible for real time applications to sustain fast secure handoffs. Our measurements are conducted under very light workload conditions. More measurements are underway to further evaluate the proposed methods for different scenarios and under different workload conditions.

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) 26-36.
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 2004).
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 2004).
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).