Fast Pre-authentication with Minimized Overhead and High Security for WLAN Handoff

Hung-Yu Chien [1], Tzu-Hang Hsu [2] and Yuan-Liang Tang[2]
[1] Department of Information management, National Chi Nan University, Taiwan
[2] Department of Information management, Chaoyang University of Technology, Taiwan
hychien@ncnu.edu.tw, http://staffweb.ncnu.edu.tw/hychien/

Abstract- User mobility in WLANs becomes more and more popular because of wide deployment of WLANs and numerous applications on it. Some of these applications, for example multimedia applications, require fast handoffs among access points to maintain the quality of service. In order to support multimedia applications for roaming users, IEEE 802.11i defines pre-authentication to reduce the re-authentication delay. The primary drawback of IEEE 802.11i pre-authentication is that the full 802.1x/EAP authentication consumes too much overhead. In this paper, we propose a new fast pre-authentication scheme that greatly improves the efficiency and achieves high security level.

Key Words: Pre-authentication, fast handoff, wireless security, IEEE 802.11i.

1. Introduction

In recent years, wireless networks based on the IEEE802.11 standard (WiFi) [11], have gained a lot of popularity, due to its low cost and high data rate. Although the data rate is very high, re-authentication during handoff procedures causes a long handoff latency which affects the Qos for multimedia applications.

In the context of IEEE 802.11 WLANs, the term handoff refers to a mobile host (MH) moves its association from one access point (AP) to another. Logically, a wireless handoff consists of probe, 802.11 authentication, re-association, and 802.11i re-authentication. In the probe phase, the MH attempts to identify a candidate set of APs via active or passive scanning. As soon as the candidate set of next APs has been identified, the MH selects one from the set of next APs. Next, the MH begins the re-association phase with the selected AP. Finally, the MH performs the 802.11i re-authentication with the selected AP. Two primary contributors to the handoff delay are the probe phase [4] and the 802.11i re-authentication phase [2].

Supporting multimedia applications with continuous mobility implies that total latency (Layer 2 and 3) of handoffs between access points has to be small. Specifically, the overall latency should not exceed 50 ms. Previous studies on latencies for WLAN have shown that 802.11i re-authentication latencies are of the order of 1s [2]. These delays are unacceptable for multimedia applications.

To reduce the handoff latency, many schemes (FHR, Neighbor Graph, DSTPA and key distribution schemes) have been proposed [1-5, 7, 13-15] to reduce 802.11i re-authentication delay. Although fast re-authentication is achievable in practice by pre-authentication [14, 15] or by proactive key distribution [2, 5, 7, 13], the prime challenge consists in achieving these at low cost. These schemes [2, 5, 7, 13-15] require an authentication server to pre-distribute the Pairwise Master Keys (PMK) for fast re-authentication. It is obvious that, as the number of users increase, the message overhead in the key pre-distribution process would become the primary bottleneck. Moreover, the previous schemes own other weaknesses that include (1) weak security due to reused PMK keys and (2) the high computational cost and storage cost for predicting the users' mobility.

In order to support multimedia applications for roaming users, IEEE 802.11i [9] defined pre-authentication to reduce the re-authentication delay. A MH can initiate pre-authentication whenever it has completed the four-way handshake and association with an AP. To initiate the pre-authentication, the MH sends, via the old AP (associated currently), an IEEE 802.1x EAPOL-Start message with the BSSID of the new AP (targeted AP). A successful pre-authentication will derive a new PMK. The MH and the new AP must cache the new PMK, and then they only perform the four-way handshake when the MH associates with the pre-authenticated AP. IEEE 802.11i pre-authentication mechanism facilitates fast re-authentication, and does not require complex algorithms to predicting the user mobility patterns.

But the primary shortcoming is a full 802.1x/EAP authentication for pre-authentication incurs high message overhead among MH, AP and AS.

To solve the high message overhead of IEEE 802.11i pre-authentication, Jan and Huang [1] proposed a fast pre-authentication scheme (which is called FPA scheme in this paper). In this scheme, when the MH sends an IEEE 802.1x EAPOL-Start message with the BSSID of the new AP to the old AP, the new AP and old AP will establish a secure channel through the assistance of the AS, and then the old AP transmits the current PMK to the new AP. Subsequently, the MH and the new AP only perform the four-way handshake when it transfers to the new AP. The FPA scheme requires less overhead, compared to 802.11i pre-authentication scheme. However, in the FPA scheme, the new AP reuses the old PMK from the old AP. So the FPA scheme has weaker security, since a compromised, old PMK key will compromise the new sessions in new APs.

It is desirable that a pre-authentication and fast handoff scheme for WLAN should simultaneously satisfy both efficiency and high security requirement. In this paper, we shall propose a new fast pre-authentication scheme to achieve secure fast roaming with less overhead. Our scheme not only greatly improves the efficiency but also achieves high security requirements.

The rest of the paper is organized as follows: Section II presents a brief background on the IEEE 802.11 handoff process. The related works are discussed in Section III. Section IV proposes our protocol, which is followed by the security analysis and the performance evaluation in Section V. This paper concludes in Section VI.

2. Background

2.1 IEEE 802.1x port-based control

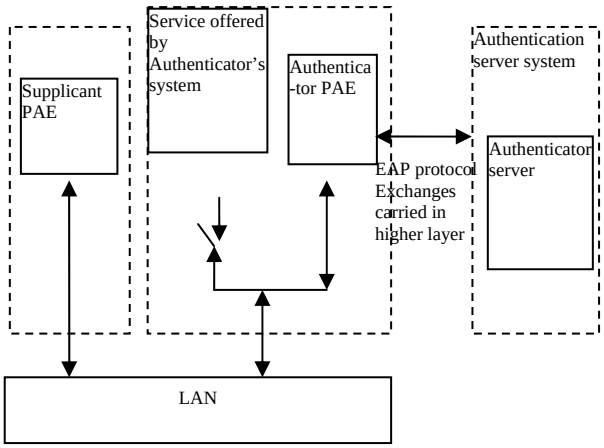

Figure 1. IEEE 802.1x architecture [8]

The IEEE 802.1x standard [8] provides a framework to facilitate network access control at the link-layer. IEEE 802.1x has three main components: the supplicant (Client), the authenticator (Access Point) and the Authentication Server (AS). Figure 1 shows a typical IEEE 802.1x architecture. A supplicant is an entity that desires to obtain network connectivity via a port on the authenticator. An authenticator controls a set of controlled/uncontrolled ports. A supplicant authenticates itself, via the uncontrolled port of the authenticator, to the AS, and the AS will direct the authenticator to provide access service through the controlled ports if the client is successfully authenticated.

2.2 IEEE 802.11i

IEEE Task Group I (TGi) has defined an authentication framework that uses the 802.1x/Extensible Authentication Protocol (EAP) in the context of IEEE 802.11 networks. We now briefly describe the process of key exchange in an IEEE 802.11i authentication (as shown on figure 2).

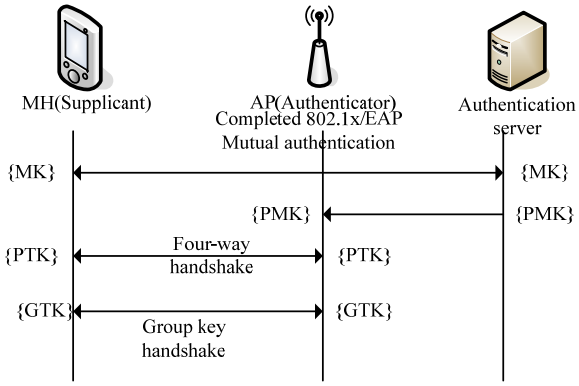

Figure 2. IEEE 802.11i pairwise key hierarchy

When the AS has successfully authenticated the MH through the IEEE 802.1x/EAP mutual authentication protocol, they will share a Master Key (MK), which will be used to derive a Pairwise Master Key (PMK), and the AS securely delivers this PMK key to the AP, through the Authentication-Authorization-Accounting protocol (AAA) protocol, for example the Radius protocol. Then, the MH and the AP can use this PMK key to authenticate each other, and perform a four-way handshake protocol to derive the Pairwise Transient Key (PTK). The AP uses the PTK to securely transmit a Group Transient Key (GTK) to the MH. The GTK is used to encrypt broadcast data to all associated MHs.

3. Related works

Jan and Huang [1] proposed the FPA scheme in 2006. This scheme assumes that each AP within the Extended Service Set (ESS) has pre-shared a secret key with the AS (RADIUS). The key idea of the scheme is based on Needham-Schroeder authentication protocol and 802.11f [10].

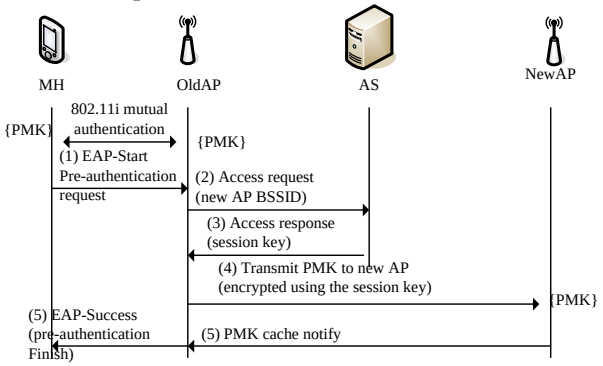

Figure 3. A pre-authentication process of FPA

The pre-authentication steps of this scheme are described below (as shown on figure 3):

1. A MH who has completed the IEEE 802.11i authentication with old AP sends an IEEE 802.1x EAPOL-Start message with the BSSID of the new AP to the old AP.
2. The old AP sends a request to the AS to request for a session key for secure communication with the new AP.
3. The AS generates a random session key. Next, the AS encrypts this session key, using the shared secret key of the old AP and the shared secret key of the new AP respectively. It finally sends the two encrypted values to the old AP.
4. The old AP decrypts and derives the session key from one of the encrypted values, and then uses this session key to encrypt the current PMK key. The old AP finally sends the encrypted PMK key and the encrypted session key to the new AP.
5. The new AP first decrypts the encrypted session key, and then uses this session key to decrypt the encrypted PMK key. Finally, the new AP notifies the old AP the successful receipt of the PMK key.
6. The old AP notifies the successful execution of the pre-authentication process.

If the above pre-authentication is successful, then the new AP and the MH will share a PMK key. Thus, only the four-way handshake is performed when the MH moves to the new AP later.

Even though this scheme can improve the efficiency of re-authentication, it incurs a security weakness: the PMK key in the current AP is reused in the next associated AP. Therefore, a compromised AP will endanger the communications of other APs.

4. The Proposed Scheme

In this section, we propose a secure fast pre-authentication scheme (which is called SFPA scheme in this paper) to improve both the efficiency and the security. This scheme consists of two phases- the fast pre-authentication phase and the fast re-authentication phase. A MH can initiate fast pre-authentication with a new AP whenever it has completed the four-way handshake and has established an association with an AP. After a successful pre-authentication, the MH and the new AP will share a secret key. Thus, when the MH moves to the new AP, they only execute the fast re-authentication process.

Secure Fast Pre-authentication (SFPA)

We assume that each AP within the Extended Service Set (ESS) has pre-shared a secret key with the AS server. Now we describe the two phases of the SFPA scheme- the pre-authentication phase and the re-authentication phase - as follows.

(1) SFPA Fast Pre-authentication Phase

The pre-authentication steps of this scheme are described below (as shown in figure 4):

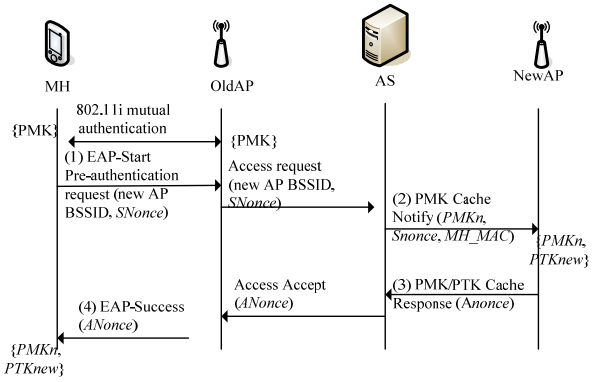

Figure 4. A pre-authentication process of SFPA

1. Once a MH has completed the IEEE 802.11i authentication with an old AP, the MH can send an IEEE 802.1x EAPOL-Start message with the BSSID of the new AP to the AS to initiate the pre-authentication phase. The EAPOL-Start message contains a MH-generated random number *SNonce* , which will be used in generating PTK key.
2. The AS uses Equation (1) to generate the new PMK_n, where PMK_0 has been generated during the full authentication process and n represents the n -th pre-authentication for

$n \geq 0$ [2]. Next, the AS uses the pre-shared key of the new AP to encrypt this PMK_n, and then forwards this encrypted PMK_n and $SNonce$ to the new AP.

$$PMK_0 = PRF(MK \| clientHell\ o.random \| serverHell\ o.random)$$

$$PMK_n = PRF(MK \| PMK_{n-1} \| AP\_MAC \| MH\_MAC) \quad (1)$$

3. The new AP decrypts the message, derives the PMK_n and $SNonce$, and then generates a random number $ANonce$. Next, the new AP uses Equation (2) to generate a new PTK_{new} and then notifies the AS the random number $ANonce$ and successful cache of the related keys.

$$PTK_{new} = PRF(PMK_n \| ANonce \| SNonce \| AP\_MAC \| MH\_MAC) \quad (2)$$

4. The AS sends, via the old AP, an Access-Accept message that contains the information of this $ANonce$ to the MH. Upon receiving the values $ANonce$, the MH can generate the PMK_n and PTK_{new} key locally.

(2) SFPA Fast Re-authentication Phase

When the MH associates to the pre-authenticated AP (the AP that has cached the PMK_n and the PTK_{new}), it can use the PMK_n and the PTK_{new} to perform Group-key handshake which requires only two message runs as shown in figure 5.

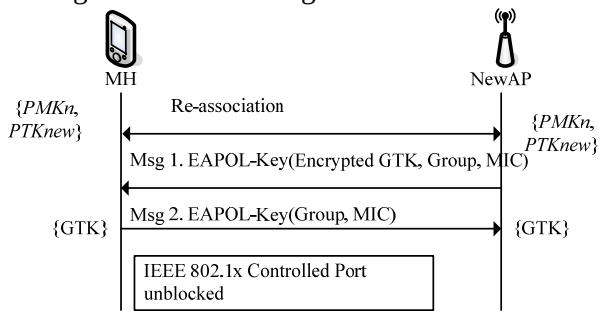

Figure 5. Group Key handshake fast re-authentication

4. Security and Performance Analysis

4.1 Security analysis

The requirements of a secure pre-authentication scheme and re-authentication should include (1) mutual authentication and fresh key derivation at each AP, and (2) minimizing delay and message overhead of both the pre-authentication phase and the re-authentication phase.

In the SFPA scheme, both the new PMK_n and the new PTK_{new} are respectively generated by AS and AP in the pre-authentication phase. The computation of PMK_n is based on MK, $PMKn$, AP_MAC, and MH_MAC, and the computation of PTK_{new} is based on PMK_n and two random numbers. Therefore, they are fresh and random for each new visited *AP*, and a compromised *AP* will not engager the security of the next *AP*. In the re-authentication, MH and AP should execute the group-key handshake protocol to mutually authenticate each other. From the above analysis, we conclude that the SFPA scheme can provide mutual authentication between MH and AP, and generate fresh and random PMK keys and PTK keys for each visited AP.

4.2 The experiment

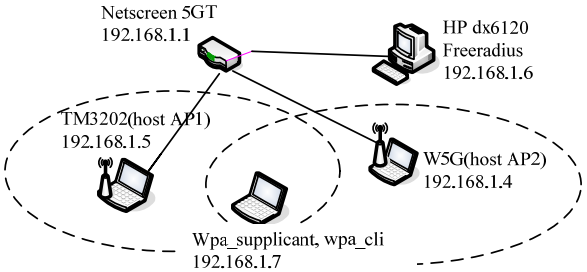

Figure 6. Experimental environment

In order to acquire practical data for evaluating the performance of our schemes, we had implemented, based on open source software, an experimental environment. The experimental network consists of two access points, a mobile host and an authentication server, as shown in Figure 6. In our experiment, we choose EAP-TLS as 802.1x authentication protocol and the RADIUS server as the AS server. The open source softwares include HostAP [17], wpa_supplicant, wpa_cli software and the Freeradius [18] software.

Evaluation of the Fast Pre-authentication Phase

We now evaluate the efficiency of our scheme in terms of the communication latency. Let $T_{MH,oldAP}$ denotes the round trip times between MH and an old AP, $T_{oldAP,newAP}$ denotes that between an old AP and a new AP, $T_{AS,oldAP}$ denotes that between AS and an old AP, and $T_{AS,newAP}$ denotes that between AS and a new AP. $T_{PMK/SK}$ denotes a PMK/Session Key

generation time at MH, AP or AS. T_{enc} / T_{dec} respectively denotes the encryption/decryption time of a message at MH, AP or AS. $T_{randNum}$ denotes the time for generating a random number at MH, AP or AS. These data can be collected from the logs of the Radius server or the HostAP. The total delay of the pre-authentication phase of the FPA scheme is $1\ T_{MH,oldAP} + 1\ T_{oldAP,newAP} + 1\ T_{AS,oldAP} + 1\ T_{PMK/SK} + 3\ T_{enc} + 3\ T_{dec}$, and that of the SFPA scheme is $1T_{MH,oldAP} + 1T_{AS,oldAP} + 1T_{AS,newAP} + 2T_{PMK/SK} + 2T_{randNum} + 1T_{enc} + 1T_{dec}$. From the logs of the Radius server and the HostAP, we obtain the following values of our environment: $T_{MH,oldAP} = 2ms$, $T_{oldAP,newAP} = 0.2ms$, $T_{AS,oldAP} = 1ms$, $T_{AS,newAP} = 1\ ms$, $T_{PMK/SK} = 6\ ms$, $T_{enc} = 1\ ms$, $T_{dec} = 1\ ms$, and $T_{randNum} = 1\ ms$.

Applying the collecting data from our environment, the 802.11i pre-authentication (using EAP-TLS) takes 380 ms, the FPA pre-authentication takes 15.2 ms and the SFPA pre-authentication takes 20 ms. The delays of the pre-authentication phases of these schemes are depicted in Figure 7. From the Figure 7, we can see that our scheme greatly improves the pre-authentication latency.

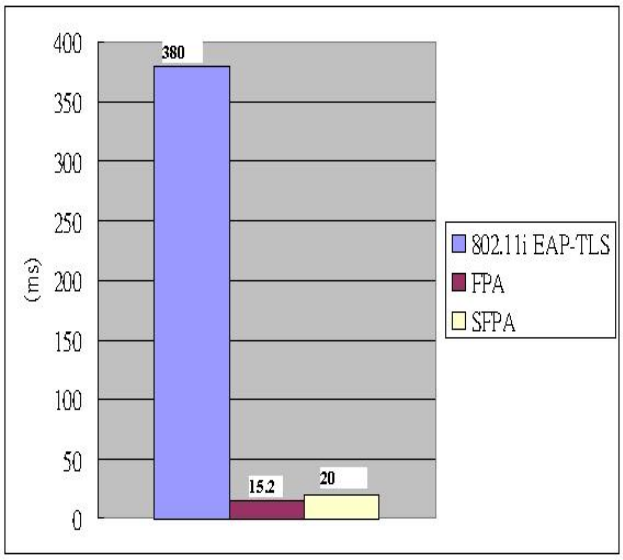

Figure 7. Fast pre-authentication latency

Overall Evaluation

This section evaluates both the communication performance and the security performance of the 802.11i pre-authentication, the FPA pre-authentication, and the SFPA pre-authentication. Since the time for generating the random numbers and the keys are almost equivalent in all the schemes and cannot be reduced, we focus on evaluating the authentication delay of various schemes. Table 1 summarizes the communication performance of the schemes. From Table 1, we can see that both our scheme and the FPA scheme greatly reduce the communication delay of pre-authentication phase.

In addition to the communication delay, we should also consider the impact of large volume of clients. Two factors will impact the performance: one is the server (AS) overhead and the other is the message overhead. Even though both FPA and SFPA need seven message rounds in their pre-authentication phases, SFPA has better performance than FPA because the AS in the FPA scheme needs to choose the random session key between the old AP and the new AP and to securely transmit the session key to them. In the re-authentication phase, FPA needs four-way handshake while SFPA needs only two-way handshake. So, as the number of clients increases, SFPA would have better performance.

Table 1. Communication performance of pre-authentication phase

scheme	The number of RTTs
802.11i Pre-Auth EAP-TLS	$5T_{MH,oldAP} + 5T_{oldAP,newAP} + 4T_{AS,newAP}$
FPA	$1T_{MH,oldAP} + 1T_{oldAP,newAP} + 1T_{AS,oldAP}$
SFPA	$1T_{MH,oldAP} + 1T_{AS,oldAP} + 1T_{AS,newAP}$

* $R_{A,B}$ **:** the number of RTTs between *A* and *B*.

Table 2. Security performance of re-authentication phases

	802.11i Pre-Auth	FPA	SFPA
Fast Re-Auth	four-way handshake	four-way handshake	Group-Key handshake
Security of newAP's PMK	High	Low*	High
Generation method of newAP's PTK	Four-way handshake	Four-way handshake	Pre-authentication

- The PMK key is reused in new APs.

Table 2 summarizes the security performance of various schemes. The re-authentication phases of both 802.11i and the FPA scheme perform the four-way handshake (four messages) process, while that of the SFPA scheme executes the two-round group-key handshake. The SFPA scheme can further improve the communication performance because it has generated the PTK key during the pre-

authentication phase. Regarding the security, the 802.11i pre-authentication and the SFPA scheme all generate fresh and random PMK keys for each AP, while the FPA scheme reuses old PMK keys at new APs. Thus, the security of the FPA scheme is weaker.

6. Conclusions

In this paper, we have analyzed the security performance and the communication performance of several previous fast handoff schemes for WLAN, and have proposed a new pre-authentication scheme. The merits of the proposed scheme include: (1) great communication performance improvement, (2) high security level- fresh and random PMK keys and PTK keys are generated for each AP, (3) no complex algorithm is required for predicting users' mobility, and (4) great improvement on reducing the load of the authentication server.

Acknowledgements
This research is partially supported by National Science Council with project number NSC95-2221-E-260-050-MY2.

References

[1] R.H. Jan and Y.C. Huang, "Fast Pre-authentication Based on IEEE 802.11i," Proceedings of the 2nd Workshop on Wireless, Ad Hoc, and Sensor Networks, Aug. 2006, pp. 317-324,.

[2] A. Mishra, M.H. Shin, N.L. Petroni, T.C. Clancy and W.A. Arbaugh, "Proactive Key Distribution Using Neighbor Graphs, " Wireless Communications, Vol. 11, pp.26-36, Feb 2004.

[3] A.R. Prasad and H. Wand, "Roaming Key Based Fast Handover in WLANs," Wireless Communications and Networking Conference, Vol. 3, March 2005, pp.13-17.

[4] 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.

[5] A. Mishra, M. Shin, and W. Arbaugh, "Context Caching Using Neighbor Graphs for Fast Handoffs in a Wireless Network," Proceedings of the IEEE INFOCOM, Vol. 1, March 2004, pp.351-361,.

[6] B. Larry and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)," IETF RFC 2284, March 1998.

[7] A. Mukherjee, T. Joshi and D. P. Agrawal, "Minimizing Re-Authentication Overheads in Infrastructure IEEE 802.11 WLAN Networks," Wireless Communications and Networking Conference, Vol. 4, pp.2334-2349, March 2005.

[8] IEEE Std. 802.1X, "Standards for Local and Metropolitan Area Networks: Standard for Port Based Network Access Control," October 2001.

[9] IEEE Std. 802.11i, "Amendment 6: Medium Access Control (MAC) Security Enhancements, " April 2004.

[10] IEEE Std. 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," July 2003.

[11] IEEE 802.11, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," June 2003.

[12] M.S. Bargh, B. Hulsebosch, H. Eertink, A.R. Prasad, P. Schoo and H. Wang, "Fast Authentication Methods for Handovers between IEEE 802.11 Wireless LANs," Proceedings of the 2nd ACM WMASH 2004, October 2004, pp.51-60.

[13] M. Kassab, A. Belghith, J. Bonnin, S. Sassi, "Fast Pre-Authentication Based on Proactive Key Distribution for 802.11 Infrastructure Networks," Proceedings of the 1st ACM WMuNeP, October 2005, pp.46-53.

[14] S. Pack and Y. Choi, "Pre-Authenticated Fast Handoff in a Public Wireless LAN based on IEEE 802.1x Model. IFIP TC6 Personcal Wireless Communications," October 2002.

[15] S. Pack and Y. Choi, "Fast Handoff Scheme based on Mobility Prediction in Public Wireless LAN Systems, IEE Proceedings Communications, " Vol. 151, No. 05, October 2004, pp. 489-495.

[16] W. Willats, P. Calhoun, "RADIUS Extensions," IETF RFC 2869, June 2000.

[17] Jouni Malinen, Host AP driver for Intersil Prism. Http://hostap.epitest.fi/

[18] Free radius, The FreeRadius Server Project. Http://www.freeradius.org.