Proceeding of the International Conference on Advanced Science, Engineering and Information Technology 2011

Hotel Equatorial Bangi-Putrajaya, Malaysia, 14 - 15 January 2011

ISBN 978-983-42366-4-9

A New Pre-authentication Scheme for IEEE 802.11i Wireless LAN Network

Rahmalia Syahputri[#+], King Sun Chan[*]

[#*] *Department of Electrical &Computer Engineering, Curtin University*
Perth, Western Australia, Australia
E-mail: rahmalia@postgrad.curtin.edu.au

+Faculty of Computer Science, IBI Darmajaya
Bandar Lampung, Lampung, Indonesia
E-mail: rahmalia@darmajaya.ac.id

***Abstract*— As 802.11 Wireless LAN network is vulnerable to many security attacks, a complicated authentication mechanism was developed in IEEE 802.11i to enhance the WLAN network security. Unfortunately, the original 802.11i authentication procedure takes some time to complete and it will significantly affect the quality of service offered to mobile users who may handover between several access points. The existing pre-authentication scheme can shorten the authentication time remarkably, but it suffers from the unnecessary signalling overhead which may be a heavy burden to the network. In this paper, we propose to improve the pre-authentication mechanism via reducing the signalling overhead. In our scheme, the mobile user will initiate the pre-authentication with a neighbouring access point only when he is really approaching that particular access point. Therefore, many unnecessary pre-authentication signalling overheads can be avoided. Preliminary simulation results show that signalling overhead can be reduced by 50% while still maintaining short authentication delay.**

Keywords— **Pre-authentication, handover, delay, cost, signal overlapping.**

I. INTRODUCTION

Security and handover are two key issues in wireless local area network (LAN) network. Security is about securely delivering data over the open wireless medium, and handover is to maintain connection while the mobile users are moving from one access point's coverage area to another access point's.

With regard to security, problems arise because wireless LAN (WLAN) networks use radio wave as the medium to exchange data and network traffic can be easily snooped by an attacker by simply launching warchalking and wardriving attacks. When an attacker can easily capture and modify the data, wireless LAN networks will lose their confidentiality, integrity and access control and the communication is no longer secure. The handover issue arises from limited coverage area of access point (AP) which is up to 300 meters [1]. This has forced users to handover to keep the connection on when moving out of the current AP's coverage area to a new one in the extended service set network, whereby the network consists of more than one AP.

In order to enable secure communication in WLAN, IEEE ratified IEEE 802.11i standard in 2004 [2]. This standard allows wireless LAN network to have secure communication through validation process applied to both the user and the device. Validation is conducted through an authentication phase and it is expected to be able to provide protection against illegal actions carried out by an unauthorized person, such as the release of a rogue AP, masquerading, man-in-the middle attack (MIMA), message modification, and Denial of Service (DoS).

The IEEE 802.11i defines IEEE 802.1X standard to control the right of devices to access the network or resources within a network. To provide authentication and key generation, IEEE 802.11 relies on Extensible Authentication Protocol (EAP) mechanism [3]. These two standards will produce a number of keys that will be used by the user, access point, and authentication server (AS) to prove their identity and build a secure communication link.

The keys are generated one by one, based on the previously generated keys. The first key is a master key which is created by AS and user or mobile node (MN) separately as a result of the completion of authentication message exchange between them. The master key is used to generate Pairwise Master Key (PMK) that will be shared between AS, MN, and AP [4]. PMK is a root key to generate other keys used to secure communications between user and AP [3]. The successful PMK is then used to derive the next key, called Pair Temporary Key (PTK). Immediately after PTK is generated, it is divided into four keys that will be used to protect the data from being tampering and protects the communication between MN and AP from MIMA attack [5].

Each time a user wishes to participate in communication in network and use its resources such as database and internet, user needs to prove that they are the person that they claim to be (an authorised person) through authentication mechanism. When an enterprise implements IEEE 80211i as its authentication mechanism, it requires a number of keys to be created and distributed. As a result, the authentication phase during handover requires a considerable amount of time. In other words, fast handover is not supported [6] and multimedia applications suffer due to the long delay [7] [8].

As mentioned in [9], efficient authentication mechanisms are required to support seamless handovers across access network boundaries. Therefore, a strong authentication mechanism is needed to provide appropriate protection against security attack. But the authentication delay should be limited to avoid degrading the quality of service offered to mobile users performing handover. At the same time, the signalling overhead introduced by authentication should also be limited. In this paper, we introduce our pre-authentication scheme which can achieve all these objectives.

The remaining of this paper is organized as follows. Section II presents a related work in this area. In Section III we explain our proposed scheme. In Section IV we present our simulation results. We conclude our paper in Section V.

II. RELATED WORK

A number of researches have been conducted in order to shorten authentication time to enable fast handoff. Pack, et al, proposed pre-authentication technique in [10] to overcome long delay in authentication processes. The basic idea is to allow MN and AAA server to exchange some authentication messages in advance, and hence some keys can be derived and then distributed to neighboring APs before MN handovers (make-before-break). The neighboring APs are a set of adjacent APs which is determined by several factors such as location of AP and users' movement pattern. The adjacent APs are named the frequent handoff region (FHR).

Link weight was introduced in [10] to determine which APs are most likely to be the next AP. The weight between APs was determined by the handoff ratio. For example, the weight of the link from AP1 and AP2 is the number of handoffs from AP_1 to AP_2 over the time spent by the MN with AP_1 before handovers to AP_2.

A particular parameter, Weight bound value (D), is used to limit the size of FHR. The total link weight of the APs included in the FHR should not be greater than D. The main issue in this scheme is how to choose D. When the value of D is high, the mobile user must perform the pre-authentication with a number of APs as the FHR will be big and hence signaling overhead will be heavy; however, if D is chosen to small, the next AP may not be included in the FHR and then the full authentication must be conducted when the mobile user handoffs which leads to long authentication delay.

The other pre-authentication scheme is introduced by Mishra, et al in [11]. They proposed Proactive Key Distribution (PKD) to distribute Pairwise Master Key (PMK) in advance to the nominated AP(s) listed in Neighbour Graph (NG). This method successfully reduced the average authentication delay from 1.1 sec to 50 ms.

There are two ways to generate the NG: it can be generated through a re-association request from MN to new AP which specifies the previous AP; or, it can be generated through move-notify message from current AP to the previous AP using Inter Access Point Protocol (IAAP).

PKD scheme modified the derivation of PMK, which was originally using the following equation:

$$PMK = TLS - PRF(MK, "client\ EAP\ encryption"| clientHello.random|serverHello.random) \quad (1)$$

The PMK was modified into:

$$PMK_n = TLS - PRF(MK, PMK_{n-1} |AP\_MAC| MS\_MAC) \quad (2)$$

Where,
n = nth re-association
$PMK_{n\text{-}1}$ = previous PMK distribution

When AS sends request to the candidate APs about a particular MN that launches a request to communicate with them, the neighbor APs can ignore or accept the request by sending a notification response. If the APs choose to grant the request, AS will send an access accept packet containing PMKn to target AP. Then the AS notifies MN by sending it the list of APs that have granted the request.

Consider topology in fig. 1, where the MN is currently associated with AP_1. In PKD scheme, AS immediately sends PMK to AP_1's neighbors (AP_2, AP_3, AP_4, and AP_5). When MN does handoff to one of the APs, say AP_2, MN only needs to perform re-association procedure. Immediately after re-association to the new AP is executed, PMK stored in AP1's other neighbours - AP_4 and AP_5 - will be deleted and AS will automatically send new PMKs to AP_2's neighbours (AP_1, AP_6, and AP_8) to facilitate seamless handover.

In fig.1, the mobile user has just done one handover from AP1 to AP2. However, many PMKs are automatically generated and distributed to many neighbouring APs like the ones distributed to AP_3, AP_4 and AP_5 which are not really needed. These unnecessary PMK derivation and distribution introduces a lot of processing and signalling overhead which may be too much if there are many handovers occurred inside the network. In this paper, we try to reduce these

overhead and hence improve the overall network performance.

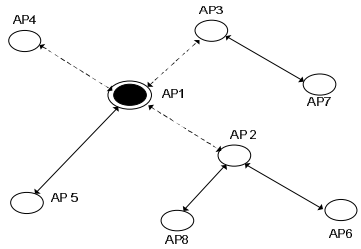

Fig. 1 Network topology and user's trajectory

III. PROPOSED SCHEME

The proposed scheme allows AS to send the PMK to target AP(s) in advance if and only if MN is approaching the target AP(s). We adopt 802.11i's EAP-TLS for authentication as it is considered as one of the strongest authentication mechanisms [4], [12] with strong mutual cryptography authentication between two end points (MN and AS) that can prevent major attack against security.

When MS approaches boundary of overlapping area between neighbouring APs which is called grey area, current AP will notify AS by sending accounting notification. Upon receiving notification from current AP, AS sends PMK in advance to APs related to the overlapping area. The AS will first send a request to the targeting AP(s). When AP(s) receives this request from the AS, it will reply by sending a notify response packet. Then the AS will send an accept packet containing PMK to the AP. If MN is static or not approaching the overlapping area, pre-authentication procedure will be not initiated.

The PMK keys will be kept for specific period (soft state time) by potential AP(s) to allow MN to move to re-association phase. When the time is over without any handover performed by MN to candidate AP, the PMK will expire and be deleted by candidate AP. This modification to initial EAP mechanism is required in order to allow pre-authentication to take place. The detail of proposed scheme is shown in fig.2.

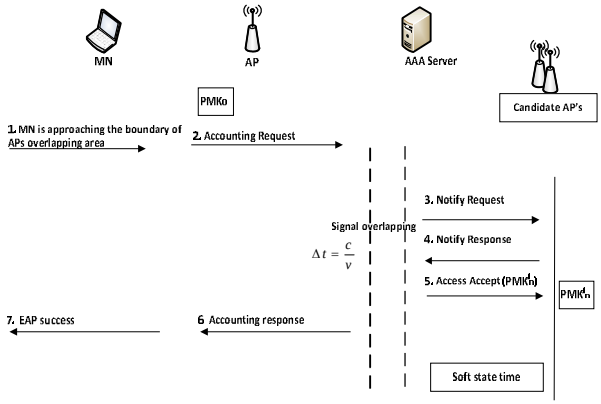

Fig. 2 Mechanism of pre-authentication

The PMK generation is modified as follows:

$$PMK_n^j = TLS - PRF\ (MK, PMK_{n-1}|nAP\_MAC|MS\_MAC) \quad (3)$$

Where:
j = potential AP
n = nth re-association
PMK_{n-1} = previous PMK distribution at APj

When MN is approaching the boundary signal overlapping with speed (v) and the coverage overlap between AP1 and AP2 is c, AS sends the key before MN cross area of c at diameter a (fig. 3) then the time to do pre-authentication (Δt) - sends the PMK - can be expressed as:

$$\Delta t = \frac{Ca}{v} \quad (4)$$

Consider the example we used before in fig. 1, the possible PMKs which may be distributed to AP1's neighbouring APs are:

AP3: $PMK_1^1 = TLS - PRF\ (MK, PMK_{n-1}|nAP\_MAC|MS\_MAC)$
AP2: $PMK_1^2 = TLS - PRF\ (MK, PMK_{n-1}|nAP\_MAC|MS\_MAC)$
AP4: $PMK_1^3 = TLS - PRF\ (MK, PMK_{n-1}|nAP\_MAC|MS\_MAC)$
AP5: $PMK_1^4 = TLS - PRF\ (MK, PMK_{n-1}|nAP\_MAC|MS\_MAC)$

After the new AP (nAP) is identified, the MN will conduct re-association with the new AP. In this step, MN only needs to tell nAP its identity to enable EAP communication to take place and to create other keys such as group temporal key (GTK) (fig. 4). MN starts re-association to the nAP immediately when the signal from the potential AP is stronger than the one from the current AP and should be completed before MN leaves the coverage area of previous AP to prevent the connection loss (fig 3).

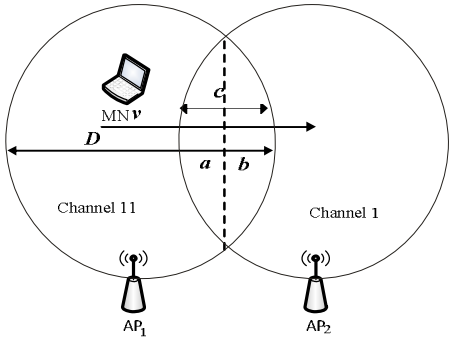

Fig.3 Time to do pre-authentication and Re-association

Hence, time to do re-association (rt) should be less than or equal to diameter of coverage area b (Db) divided by speed movement of MN (v) (fig.3).

$$\Delta rt = \frac{Db}{v} \quad (5)$$

The distributed PMK will be removed automatically when one of these two conditions is met: the soft state time is finished or MN re-associates to the new AP. This mechanism is conducted to ensure malicious MN cannot

steal the PMK. Fig. 3 shows the scheme of re-association between MN and nAP.

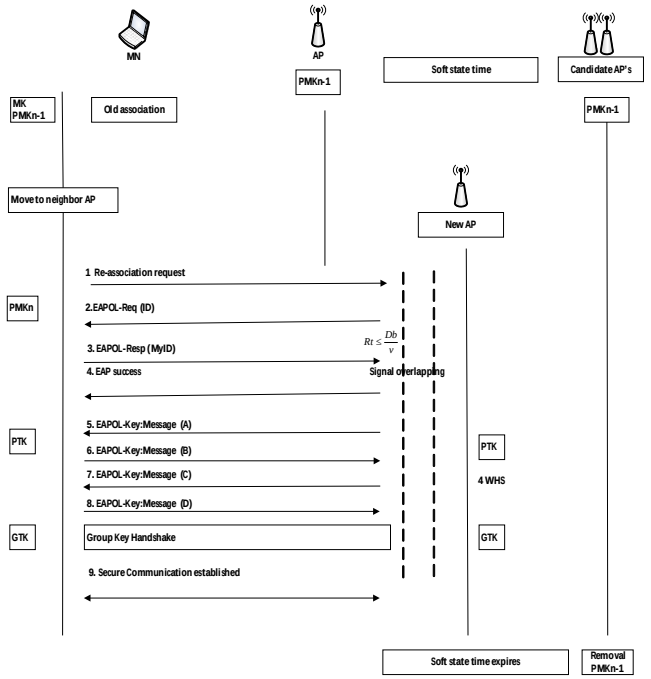

Fig. 4 Mechanism of re-association

IV. Simulation, Result, and Analysis

We use ns-2 to evaluate the performance of our scheme. IEEE 802.11g is chosen as our network model as it supports IEEE 802.11i for security. Each of AP's coverage area is 300 meters, overlapping area between APs is 100 meters, and 3 channels reusing model is adopted (fig.5). The general parameters of simulation are shown as follows:

Table 1 General parameter setting

Parameter	Value
Number of nodes	2 users, 9 APs
Radio coverage area	300 m
Topography	600 x 600 m
User Movement Speed	10 ms
Power at transmitter	0.281838
RTS threshold	1000 bytes
AP's beacon interval	0.2
MAC address	Auto

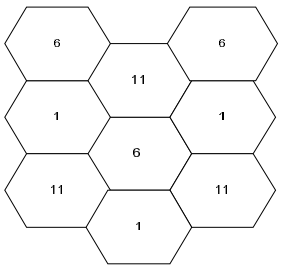

Fig.5 Channels re-use model

Topology below shows the APs' physical position and its overlapping area and MN's physical movement from first movement until fifth. However, in our simulation, eleven movements are conducted to get more accurate evaluation.

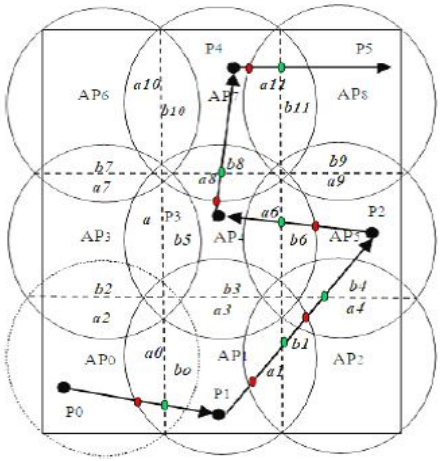

Fig. 6 Network topology and MN's trajectory

Current position of MN 1 is attached to AP_0 and sends UDP packets to a correspondent. The doted circle is the first AP that MN is connected to. The red dot color is the location where pre-authentication started to take place, because at this point the MN can hear both AP_0 and AP_1. The green dot indicates when pre-authentication should be completed and re-association to AP2 should be initiated. After a random delay, the MN starts to move through all the areas from position 0 (P_0) until position 11 (P_{11}) without pause until the simulation time is over.

Based on simulation, MN experiences 16 handovers within 11 movements. It happened because for some movements, the MN may experience two handovers, due to the distance from current positions to the next position which is far enough. Consequently, to maintain the connection, MN needs to handoff to the closet AP before it reaches the designated AP.

Based on number of handovers, the cost to pre-authenticate and re-associate can be calculated. The term of cost in this paper refers to number of message exchanges between network entities: MN, AP, and AS during the movements. For each message sent, it has a cost of ***t***. The signaling flowchart in our scheme is almost the same as the one described in the PKD scheme; the difference is about when the signaling is sent and who are involved in the signaling.

We give an example to explain how the total cost is calculated. We consider the movement of the MN from position P0 to position P1, where the MN handovers from AP0 to AP1. At position P_0, MN_1 is attached to AP_0 and starts to send UDP packets to its correspondent. At time (t0), MN starts to move to position P_1, which leads to approaching the overlapping area between AP_0 and AP_1. When the MN hears the signal from AP1, AS sends the appropriate PMK to AP_1 with cost ***7t***. When the MN finds the signal from AP_1 is stronger than the one from AP_0, the MN initiates its re-association with AP_1 with cost ***8t***. As this

is the first association, the cost will be added with full authentication which requires ***16t***. The total cost is ***31t***. Full authentication is only needed when the MN is associated with the network first time. The subsequent authentication with other APs is achieved via pre-authentication.

The total cost of each movement for our scheme and for PKD scheme is shown in fig. 7. In Fig. 8, we show the difference of signaling cost from our scheme and from PKD, when the MN is static.

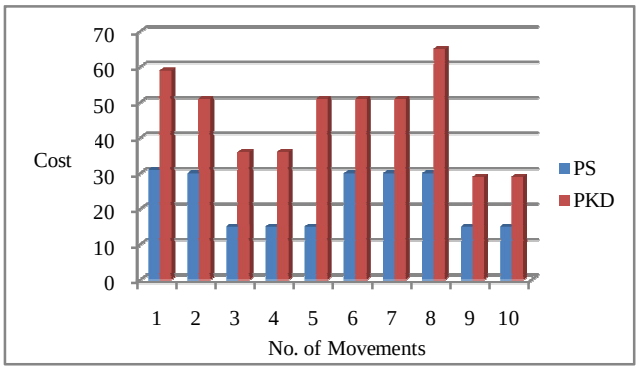

Fig. 7 Cost of PMK distribution and re-association at random movement

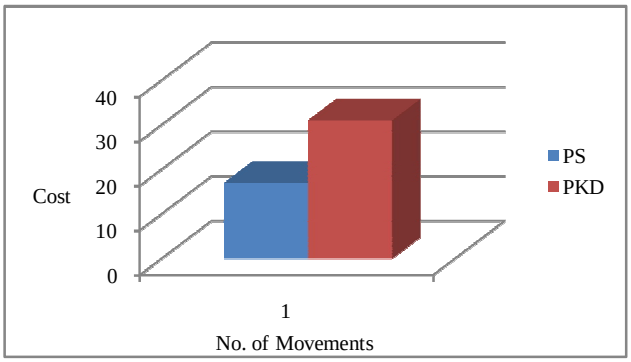

Fig. 8 Cost of PMK distribution and re-association at Null movement

From fig. 7, it can be seen that the cost of PKD scheme is higher than our proposed scheme. This is because each time new re-association is executed, the new AP or AS sends the PMK immediately to the neighbor APs, for instance a movement from P_0 to P_1. At position 0 – or known as initial connection – MN performs full authentication, then AS immediately sends the key to AP_1 and AP_3 which is considered as AP_0's neighbor. When MN moves to P_1, MN is able to re-associate directly to AP1. When re-association done, AS sends PMK to AP_1's neighbor (AP_0, AP2, and AP_4). In our proposed scheme, the AS sends the PMK in advance only when the key distribution is triggered. Thus, this act will save cost and does not keep the AS busy.

For each movement of 6, 7, 8, and 9, multiple handovers occur. Consider The MN movement from P_5 to P_6, MN first pre-authenticates and re-associates with AP_5 before finally it pre-authenticates and re-associates with AP_2. Cost for the proposed scheme is only half of the PKD scheme.

Fig.8 shows the cost when MN does not do any movement and keeps its connection to the current AP (AP_0). The proposed scheme shows that the cost occurs only at the initial authentication, the PKD scheme cost is higher because AS sends the PMK to NG though MN is static.

V. Conclusion

The 802.11 wireless LAN network is vulnerable to many security attacks. Authentication is a promising mechanism to enhance security for wireless LAN network. Unfortunately, the standardized 802.11i authentication mechanism introduces a long delay which may degrade the quality of service received by mobile users. Pre-authentication scheme like PKD can shorten the authentication delay significantly but suffers from heavy unnecessary signalling overhead as it requires to pre-authenticate with all neighbouring access points. In this paper, we propose to initiate the pre-authentication only when it is necessary and therefore reducing the signalling overhead and still maintains short authentication delay. Simulation results show that our scheme can reduce the signalling overhead by almost 50%.

REFERENCES

[1] Cisco Networking Academy Program. (2004).“Fundamental of Wireless LANs Companion Guide”. Cisco Press.

[2] He, Changhua., Mitchell., John C . (2005) "Security Analysis and Improvements for IEEE 802.11i". Proceedings of the 12th Annual Network and Distributed System Security Symposium.

[3] Frankel, Sheila., Eydt, Bernard., Owens, Les., Scarfone, Karen. (2007). "Establishing Wireless Robust Secure Network: A Guide to IEEE 802.11i". National Institute of Standards and Technology, Technology administrations U.S, Department of Commerce, Special Publication 800 - 97.

[4] Aboba, Bernard D, Simon. (1999).” PPP EAP TLS Authentication Protocol”. RFC 2176. http://www.ietf.org/rfc/rfc2716.txt

[5] Edney, Jon., Arbaugh, A.William. (2004). " Real 802.11 Security: Wi-Fi Protected Access and 802.11i". Addison Wesley.

[6] Marques, Rodolphe., Zuquete, Andre. (2008). "Fast, Secure Handovers in 802.11: Back to the Basis". Proceedings of the 4th ACM symposium on QoS and security for wireless and mobile networks , pp 27 - 34.

[7] Pack, Sangheon., Choi, Jaeyoung., Kwon, Taekyoung., and Choi, Yanghee. (2007). Fast Handoff Support in 802.11 Wireless Network". IEEE Communication Survey and Tutorial.

[8] Lopez, R., Dutta, A., Ohba, Y., Schulzrinne, H., and A. Skarmeta. (2007). "Network-layer Assisted Mechanism to Optimize Authentication Delay During Handoff in 802.11 Networks". The 4th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services.

[9] Wienzek, Ralf., Persaud, Rajendra, (2006). Fast Re-authentication for Handovers in Wireless Communication Networks". Networking 2006, LNCS 3976, pp. 556–567.

[10] Pack, Sangheon., Choi, Yanghee. (2002). "Fast Handoff Scheme Based on Mobility Prediction in Public Wireless LAN System". in Proc. IEEE Networks 2002 (Joint ICN 2002 and ICWLHN 2002), Atlanta, USA.

[11] Mishra, Arunesh., Shin, Minho., and Arbaugh, William.,(2004). "Pro-active Key Distribution using Neighbor Graphs". IEEE Wireless Communications February 2004.

[12] Earle, Aaron E. (2006). "Wireless Security Handbook". Auerbach Publications.