Multiple preauthentication schemes based on fast channel switching in public Wireless LANs

JaeJong Baek, JooSeok Song
Department of Computer Science
Yonsei University, Seoul, Korea
E-mail: {jjb27, jssong}@cclab.yonsei.ac.kr

SungHoon Seo
Department of Computer Science
Columbia University, NY, USA
E-mail: hoon@cs.columbia.edu

Abstract

Seamless handoff issues including authentications have become considerable interest in wireless networks, which support pervasive environment users. Usually the active scanning and preauthentication methods are adopted to solve the disruption in seamless services. In this paper, we propose a new preauthentication scheme based on the fast channel switching and the power saving mode (PSM) in public wireless local area networks (LANs). We prove the effect of our proposed scheme using the simulation programming results. During the channel switching period (CPS), our proposed scheme performs multiple preauthentication with pre-scanned neighbor Access Points (APs). By using very short period of channel switching, our scheme doe not degrade Quality-of-Service (QoS) of its current applications. It also reduces the authentication latency in handoffs and improves the random mobility of users. In addition, our scheme only requires minor implementation changes on the client device driver, so it is apt for being deployed in current WLANs environment.

1. Introduction

Although many WLANs′ APs have been deployed in the recent years, we have faced the disruptions in the connectivity when an STA (station) conducts a handoff or roaming procedure. A handoff occurs when an STA moves beyond the radio range of one AP, and enters another Basic Service Set (BSS). The handoff procedure consists of four phase: scanning, joining, authentication and association. The scanning phase is notably well known to consume approximately 90% of the handoff time [1]. Many studies have been worked to reduce the latency in scanning phase but the authentication latency has been considered as a trivial concern [3, 4]. However, as the network environment changes to be heterogeneously internetworked, various link layer authentication protocols such as 802.1X/EAP (Extensible Authentication Protocol) are emerging in various handoffs. It means that the different authentication protocols can be the disruptions during the handoff procedure. Table 1 shows the complicated message signaling costs [5]. Until recently, little research has been done on reducing the latency of authentication phase in handoffs. However, we have focused on reducing the latency of authentication phases by the fast channel switching scheme and a power saving mode of the 802.11.

Table 1. Messages cost in EAP protocols

EAP-AKA	SIM-based EAP-AKA	EAP-UTLS	Robust Authentication protocol
9a+12b	5a+9b	10a+10b	6a+8b

*a: signaling messages between STAs and APs
*b: signaling messages between network nodes
*EAP-AKA: EAP-Authentication Key Agreement
*SIM: Subscriber Identity Module
*EAP-UTLS: EAP Tunneled TLS

The key idea of our scheme is to perform the preauthentication with all neighbor APs, which are scanned previously. It will be performed when the STA is in idle state or not. During the short switched channel time, a few messages will be exchanged between STAs and APs. This specific time period is allocated to the STA's MAC (Media Access Control) layer for processing some procedures such as EAP request/response. The function of PSM will provide the STA with the time to process the current task at the same time. Thus, STAs' current tasks do not experience the degrading of QoS. Therefore, the fast channel switching-based preauthentication with PSM

978-1-4244-5700-7/10/$26.00 ©2009 IEEE

improves the handoff seamlessly and the random mobility of mobile stations. The random mobility means the random mobile direction of user which cannot be predicted. Thus, we provide multiple preauthentication with all neighbor APs, which are scanned previously. In this way, the users can move to any place they want to. Our scheme only requires trivial implementation changes on client side, which is advantageous to the deployment. The rest of the paper is organized as follows. In section 2, we review the related work such as IEEE 802.11i preauthentication and MultiNet. Section 3 describes our proposed scheme with message flows and algorithms. We present the result of simulation related to predict Listen Interval (LI) in section 4. Finally, we conclude the work in Section 5.

2. Related work

.

2.1 Solutions for intra-technology handoff

For the IEEE 802.11s' intra-technology handoff, several solutions are available typically within the same Authentication, Authorization and Accounting (AAA) domain. IEEE introduces preauthentication defined in 802.11i [6] and fast BSS transition defined in 802.11r [7] for inter-AP WLAN handoff. The main goal of these solutions is to reduce the time to perform EAP-based network access authentication. In IEEE 802.11i, if the STA knows where it will roam, it will conduct the preauthentication to a new target AP. The preauthentication packets will be sent to the target AP through the current AP. The preauthentication provides a way to establish a security association before an STA associate with a new AP. Fast BSS Transition of the IEEE 802.11r can reduce not only the transition time but also the packet loss during an STA's roaming between two APs in an 11r-enabled network. When the STA roams to the target AP, it can perform the fast BSS transition by sending reassociation request without performing additional authentication procedures such as IEEE 802.1X authentication.

2.2 MultiNet

MultiNet defines virtualization of a network interface card (NIC) as an abstraction of multiple wireless networks. It uses an adaptive network hopping scheme where an NIC gets a time slot, called the Activity Period. MultiNet uses the PSM in IEEE 802.11 for seamless service and a switch mechanism by allocating the time slot to STAs. However, it cannot be directly applied to handoff scenario for two reasons. One is that the network information is not known before scanning. The other is that how to connect to multiple APs is not addressed in MultiNet [3].

3. Proposed Scheme

The multiple preauthentication means that the STA can be authenticated with many APs before the handoff. The reason of handoffs has two scenarios. First, the movement of users or STAs will be the main reason for an STA to handoff. Second, the new AP with the better RSSID (radio signal strength indicator) is emerging around the STA. Likewise; the handoff trigger will be caused by any of the two reasons mentioned above. Our key idea is to perform the preauthentication with all or selective pre-scanned neighbor APs using the fast channel switching and PSM operations before handoffs.

3.1 Preauthentication using PSM

In preauthentication between STAs and APs, we use the PSM feature available in IEEE 802.11 networks. The STAs will pretend to be the PSM to the APs when they switch to a new AP for sending any messages. When an NIC enters PSM, the AP automatically buffers packets for that NIC. Although the AP considers that the STA is sleeping, the STA actually switches and is actively connected to new AP. After the sleep interval, the NIC listens to the beacon. If the new AP has the buffered frames for the STA, it sends a beacon frame containing the traffic indication virtual bitmap (TIM) element. If the STA determines that frames are buffered for it, it sends a power save poll (PS-Poll) frame and receives the buffered packets. The function of PSM will provide the STA with the time to process the current task at the same time. Thus, STAs' current tasks do not experience the degrading of QoS.

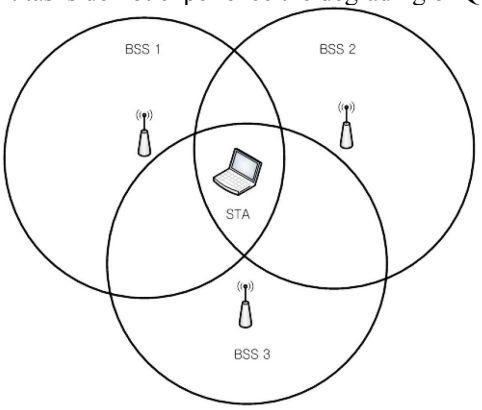

Figure 1. STAs in overlapped coverage environment

If so, the STA will be able to connect with the new AP in a very short delay. In addition, it is not necessary to limit the movement of users because all APs are authenticated previously. As shown in Figure 1, we assume four conditions in network environment. First, an STA is in the coverage area of three different APs. Second, through the active and passive scanning mechanisms [3] or any other discovery approaches, we assume that the STA has already known the neighbor APs with the state information such as RSSID, beacon interval (BI), and channels etc. Third, we also assume that the contention window between STAs is not considered in this scheme. Lastly, the WLANs' service providers are different from each other.

3.2 Basic procedure

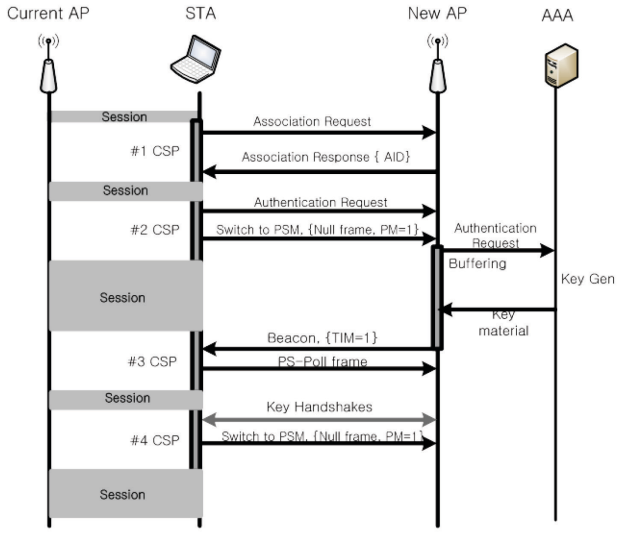

Figure 2. Proposed scheme procedure

As shown in Figure 2, we assume that the STA is connected to one AP and the channel switch period (CSP) is able to be allocated to the STA. The new AP was also scanned and selected by the STA previously. The station authentication process (open and shared-key) is omitted, because our proposed scheme is applied to the 802.1X/EAP link layer authentication mechanisms. The one additional assumption is that the STA must wake up at LI. As we mentioned, we adopt the buffering scheme of 802.11 PSM for receiving the result of preauthentication. The STAs will pretend to enter PSM to the APs when they switch to the new AP for sending any messages. The AP buffers frames destined for the station while the STA is in PSM. During being in the PSM, the STA processes its current tasks. After the sleep interval, the NIC connects to the AP and receives all the buffered packets which contain expected response from AAA server or network. The proposed preauthentication mechanism is described as follows:

1. While the STA is connecting to the current AP, #1 CSP is allocated by the STA itself.
   i) The STA attempts to associate with the new AP.
   ii) The listen interval (LI) is specified in the association request frame. LI indicates the time by which the STA is waken up periodically to receive buffered frame
2. When the association request is granted,
   i) The AP responds with the Association ID (AID). A STA can only be associated with a single AP, so this additional AID must be included in the table.(see Table 2)
3. In # 2 CSP, the STA requests authentication to the new AP with a link layer authentication protocol such as EAP-AKA.
   i) The STA enters PSM and is waken up by the beacon from new AP.
4. When the AAA receives the authentication request from the new AP,
   i) Dynamic keys are derived from both sides through the four-way handshake or group key handshake.
   ii) The results of this process are buffered into the new AP.
   iii) In every 100 msec of LI, the STA listens to the beacon frame from the new AP, and checks whether the response of authentication has arrived or not.
5. In # 3 CSP, if the new AP has the STA's AID in TIM filed
   i) The STA sends PS-Poll frame to the new AP
   ii) The STA receives the response result and completes authentication process.
   iii) Otherwise # 5 phase is repeated.
6. In #4 CSP, if the STA completes the authentication process, it enters PSM again.

Table 2. Key cache table example

Channel #	BSSID	AID	KEYn…
3	0x 002275 02FADD	1	0xFFFF

The flow of our proposed scheme is shown in Figure 3. The new AID will be stored with other association parameters in a table as shown in Table 2. This state table is for retaining multiple associations and it makes a faster reconnection by using reusable information of connection in the next time. The CSP means channel switch period for sending messages to the new AP. Figure 2 shows that 4 CSPs are needed, but it depends on the result of authentication.

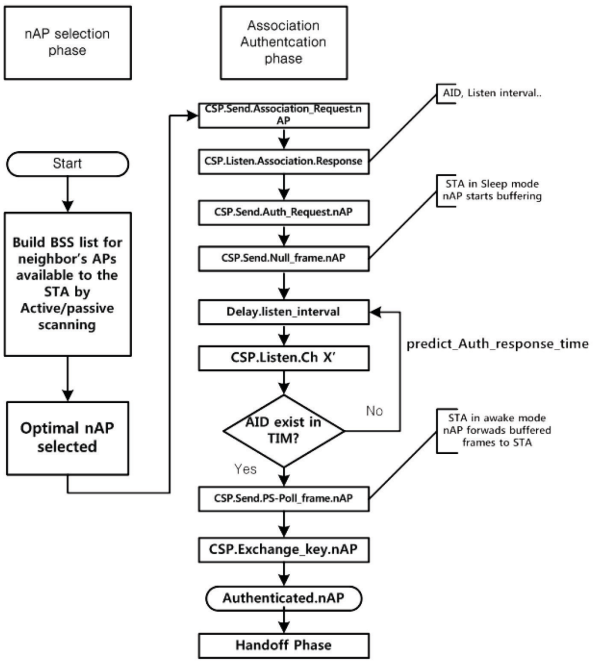

Figure 3. Flow of the proposed scheme

3.3 Prediction methods of the arrival time

In our proposed scheme, the key function is to predict the arrival time from AAA servers to APs. The purposes of predicting the accurate arrival time are to improve energy efficiency and to reduce network overheads. In order to support the prediction, we approach predicting the response time in two ways. The first way is to employ the fixed time of the minimum period of the listen interval (100 msec [2]). The other way is to employ the mean queuing time in AAA servers. Hence, the prediction of arrival time is the key role to prevent the STA from wasting energy and frame overhead. Figure 4 shows our simulation model, STAs request authentication to AAA server through an AP. We assume each value as follows:

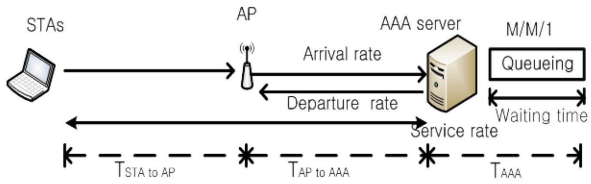

Figure 4. Simulation model

- $T_{Expected\ Response} = T_{STA\ to\ AP} + 2 \times T_{AP\ to\ AAA} + T_{AAA}$
- $T_{STA\ to\ AP} = T_{STAch\_switch\_time} + T_{Null/PS\text{-}poll\ message}$
- $T_{AP\ to\ AAA} = T_{Network\ propagation\ delay}$
- $T_{AAA} = T_q = T_w + T_s$

$T_{Expected\ Response}$ denotes the expected response time and consists of $T_{STA\ to\ AP}$, $2 \times T_{AP\ to\ AAA}$ and T_{AAA}. $T_{STA\ to\ AP}$ is the delay time from STAs to APs. $T_{AP\ to\ AAA}$ is the delay time from APs to AAAs. T_{AAA} (time to process in AAA) is the same value of T_q which is the mean queuing time and consists T_w (time to wait) and T_s (time to serve). We assume that $T_{STA\ to\ AP}$ and $T_{AP\ to\ AAA}$ values are the constant value because of the network propagation time. Meanwhile, T_{AAA} can have various random values according to the service rate and the situation of AAA server such as the number of waiting STAs. Thus we only need to know the random value, T_{AAA}.

4. EVALUATION BY SIMULATION

The two prediction methods have been studied by simulations where 10 STAs request preauthentication to the same AP randomly. We modeled the AAA server's queue as M/M/1 queuing model with SMPL simulation library [8]. For the simulation input parameters, the mean inter-arrival time Ta is 200 msec, the mean service time Ts is 100 msec, and the default LI is 100 msec. As a result, the utilization (ρ) is 0.7179 as shown in Figure 5.

MODEL: M/M/1 Queue

TIME: 2171.674
INTERVAL: 2171.674

FACILITY	UTIL.	MEAN BUSY PERIOD	MEAN QUEUE LENGTH	OPERATION COUNTS RELEASE	PREEMPT	QUEUE
server	0.7179	155.909	0.223	10	0	5

Figure 5. Simulation result report

The mean queuing time T_q is given by Lttle's formula:

$$T_q = \frac{T_s}{1-\rho} \cong 354m\sec \quad (1)$$

Where T_s is the mean service time and the ρ is the utilization of the queuing system. Based on the T_q in formula (1), the mean queuing time is approximately 354 msec, which is applied to the optimal listen interval in our simulation.

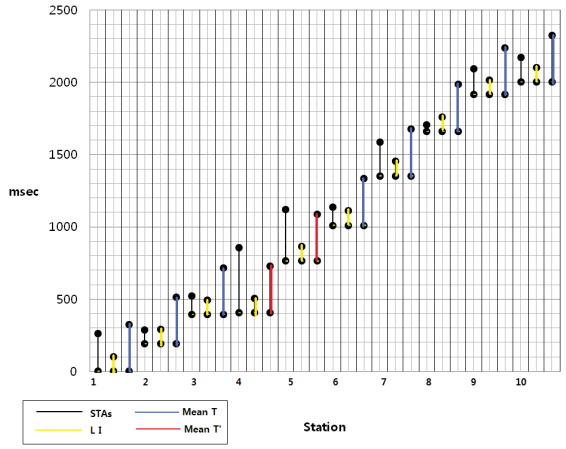

Figure 6. Simulation Result

Figure 6. shows the simulation result. The first black line denotes the first STA's arrival and departure time, the second yellow line denotes the default LI (100 msec) time line, and the third blue or red line denotes the default LI including the mean queuing time (354 msec). If the STA checks at the second LI (yellow line) in the case of STA1, it will fail to receive its frame. However, if STA1 checks at the 3rd blue line, STA1 can receive its frame form AP successfully. AS the same way, except STA 4 and 5, the rest 8 STAs can successfully receive their frames from the AP. In the case of the default LI, only STA 2 and 8 can success. As a result, if the STA waits for the LI including mean queue length of AAA server, the efficiency will be improved 4 times.

5. Conclusion

In this paper, we proposed a new preauthentication mechanism to reduce the authentication latency and the predicting methods for the response time from authentication servers. When the STAs enter an overlapped coverage area, using the fast channel switching period, the STA can associate and authenticate the scanned multiple neighbor APs. By doing this, when the STA performs handoff, the authentication latency will be reduced dramatically. Lastly, we proved that employing the mean queuing time of AAA server in predicting the response time is better (approximately four times) than employing the default LI for receiving the buffered frames from AP. In the future, we will implement our scheme in a commercial 802.11 hardware. Additionally, predicting more appropriate LI in any situation and decreasing energy consumption will be further studied.

6. Acknowledgement

This work was supported by the Korea Science and Engineering Foundation (KOSEF) grant funded by the Korea government (MEST)(2009-0076476).

7. References

[1] A. Mishra, M. Shin, and W. Arbaugh, .An Empirical Analysis of the IEEE 802.11 MAC layer Handoff Process,. University of Maryland, College Park, Tech. Rep. UMIACS-TR-2002-75, Nov 2002

[2] Wireless LAN medium access control (MAC) and physical layer(PHY) specifications. IEEE std, 802.11., 1997

[3] H. Wu, K. Tan, Y. Zhang, and Q. Zhang. Proactive scan: Fast handoff_ with smart triggers for 802.11 wireless LAN. pages 749-757, 2007.

[4] R. Chandra and P. Bahl. MultiNet: Connecting to multiple IEEE 802.11 networks using a single wireless card. In INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, volume 2, 2004.

[5] S. Jung · J. Ahn, A Survey of USIM-based Authentication Mechanisms for Vertical Handover in FMC Network s, Telecommunication Review, vol 35-8, 8, 2008

[6] IEEE 802.11r: Fast Roaming/Fast BSS Transition. http://www.ieee802.org/11/

[7] IEEE Std 802.11i-2004: IEEE Standard for Information technology – Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access