Pre-Authenticated Fast Handoff in a Public Wireless LAN based on IEEE 802.1x Model[1]

Sangheon Pack and Yanghee Choi
School of Computer Science & Engineering, Seoul National University, Seoul, Korea
Telephone: +82-2-880-1832, Fax: +82-2-872-2045, E-mail: {shpack, yhchoi}@mmlab.snu.ac.kr

Abstract: With the popularity of portable devices, public Internet access service using wireless LAN has started in many countries. In the public wireless LAN network, since re-authentication latency during handoff affects the service quality of multimedia applications, minimizing authentication latency is very important in order to support real-time multimedia applications on the wireless IP network. In this paper, we proposed a fast handoff scheme using the predictive authentication method based on IEEE 802.1x model. In our scheme, a mobile host entering an area of an access point (AP) performs authentication procedures for a set of multiple APs instead of the current AP. Multiple APs are selected using a Frequent Handoff Region (FHR) selection algorithm considering users' mobility patterns and their service classes. Since a mobile host is authenticated for FHR in advance, the handoff latency due to the re-authentication can be minimized. Simulation results show that the proposed scheme is more efficient than other schemes in terms of delay.

Key words: Wireless LAN, Fast Handoff, Authentication, FHR, IEEE 802.1x

1. INTRODUCTION

Public wireless Internet services based on IEEE 802.11 wireless LAN technology are becoming popular in hot spot regions such as hotels, airports, shopping malls, and so on. Unlike the existing wireless Internet service, the public wireless LAN system can provide fast Internet access at speeds up to

[1] This work was supported in part by the Brain Korea 21 project of the Ministry of Education, and in part by the National Research Laboratory project of Ministry of Science and Technology, 2002, Korea.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35618-1_37
C. G. Omidyar (ed.), *Mobile and Wireless Communications*

11Mbps using portable devices such as laptop computers and Personal Digital Assistances (PDA). In this public wireless LAN system, the user authentication and mobility support between Access Points (AP) are one of the critical issues.

To overcome some drawbacks of the existing authentication scheme, IEEE has suggested an alternative authentication scheme based on the IEEE 802.1x model [1]. In IEEE 802.1x, a network-to-client authentication mechanism utilizing EAP (Extensible Authentication Protocol) is used as the encapsulation protocol for upper-layer authentication information [1]. Since IEEE 802.1x provides a network port access control scheme, it is more scalable and robust than other schemes. The authentication mechanism may impact network and device performances. Because mobile hosts should to be authenticated during and after handoff, the used authentication mechanism need to be responsive to the handoff time-scale required in micro-mobility environments [2]. However, since AAA servers are located at locations far away from the AP, current handoff schemes cannot meet all requirements of the real-time multimedia applications.

In this paper, we propose a fast handoff scheme that minimizes the authentication latency in a public wireless LAN. This algorithm is a centralized method based on traffic patterns and user mobility characteristics. In terms of architecture, we assume that the public wireless LAN system is based on IEEE 802.1x and uses IETF standard authentication servers. The remainder of this paper is organized as follows. Section 2 outlines the IEEE 802.1x model. In Section 3, we propose the fast handoff scheme using FHR selection. Section 4 describes the simulation results. Section 5 concludes this paper.

2. BACKGROUND

In this paper, we assumed a public wireless LAN architecture based on the 802.1x model [1]. Fig. 1 shows the basic components and the port-based access control mechanism. The *Supplicant system* is an entity at one end of a point-to-point LAN segment that is being authenticated by an Authenticator attached to the other end of that link. The *Authenticator system* is an entity at one end of a LAN segment that facilitates authentication of the entity attached to the other end of that link and the *Authentication server system* is an entity that provides an authentication service. Port Access Entity (PAE) is the protocol entity associated with a port.

In Fig. 1, the Authenticator's controlled port is in the unauthorized state and is therefore disabled from the point of view of access to the services offered by the Authenticator's system. The Authenticator PAE makes use of

the uncontrolled port to communicate with the Supplicant PAE, using EAPOL protocol exchanges, and communicates with the Authentication Server using Extensible Authentication Protocol (EAP). The communication between the Authenticator and the Authentication Server may make use of the services of a LAN. The public wireless LAN architecture based on 802.1x is in Fig. 2. In this architecture, the Supplicant is a user host requesting the authentication and moving from one AP to another AP. The corresponding AP and AAA server play the roles of Authenticator and Authentication server, respectively.

Recently, new authentication scheme for fast handoff is proposed [3]. This is called preauthentication scheme. In this scheme, stations can authenticate with several APs during the scanning process so that when association is required, the station is already authenticated. As a result of preauthentication, stations can reassociate with APs immediately upon moving into their coverage area, rather than having to wait for the authentication exchange. Preauthentication makes roaming a smoother operation because authentication can take place before it is needed to support an association. However, since this scheme doesn't predict where the MH moves in the future, the preauthentication may be useless in some cases and cause unnecessary authentication procedures in the wireless link.

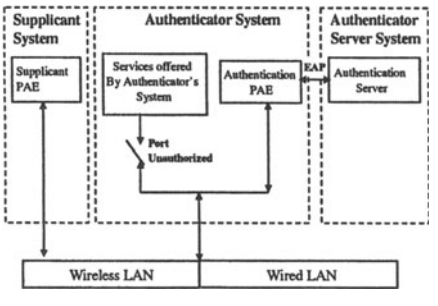

Fig.1. Port-based authentication scheme

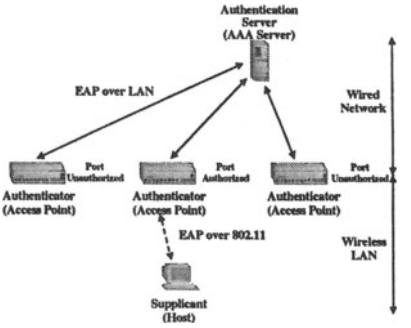

Fig. 2. The basic IEEE 802.1x architecture

3. PRE-AUTHENTICATED FAST HANDOFF

In this section, we propose a fast inter-AP handoff scheme. In the scheme, a mobile host performs authentication procedures not only for the current AP but also for neighboring APs (Frequent Handoff Region), when it handoffs.

3.1 Frequent Handoff Region (FHR) Selection

The FHR is a set of adjacent APs. It is determined by the APs' locations and users' movement patterns. Namely, the FHR consists of APs with which mobile hosts are likely to communicate to in the near future. Although there are a lot of APs in a public wireless LAN, the movement ratios between each AP are not same. The handoff probability for specific APs can be calculated by the movement ratio. The movement ratio is usually affected by the AP's location and user mobility. For example, if two APs are installed within a large conference room, users may move from one AP to another AP frequently and the movement ratio will be high. However, if there are some obstacles between the APs, users will seldom move between the APs. Therefore, to find the correct movement ratio between APs, these factors should be considered.

To measure movement ratio between APs, event logging database system can be used. Table 1 shows an example of a database that records the users' login and handoff events.

Table 1. Example of Event Log Database

Number	User ID	Login Time	Handoff Time	Handoff Time
1	2314	07:54:57/3		
2	3452	08:00:55/2	08:05:18/5	
3	1093	08:04:23/3	08:14:03/6	08:15:17/4

After recording the events, we should find out the handoff ratio between APs. The handoff ratio is calculated in Eq. (1) using information in the event database.

$$H(i, j) = \frac{N(i, j)}{R(i, j)} \tag{1}$$

$H(i, j)$ and $N(i, j)$ denote the handoff ratio and the number of handoff events from AP(i) to AP(j), respectively. $R(i, j)$ denotes the residential time in AP(i) of handoff events from AP(i) to AP(j). The weight values between APs are determined by the handoff ratio. Eq. (2) shows the weight value function between AP(i) and AP(j). $w(i, j)$ denotes the weight value.

$$w(i, j) = \begin{cases} 0 & (i = j) \\ \dfrac{1}{H(i, j)} & (i \neq j,\ AP(i)\ and\ AP(j)\ are\ adjacent) \\ \infty & (AP(i)\ and\ AP(j)\ are\ \text{not}\ adjacent) \end{cases} \tag{2}$$

As in Eq. (2), the weight value is inversely proportional to the handoff ratio. The weight value in the path from AP(i) to AP(i) is set to zero and the weight value between non-adjacent APs is infinite. To select the FHR, the user's service level as well as its mobility pattern should be considered. Some users may be satisfied in spite of the session disconnection during handoff. But, other users may want more seamless connectivity without any data losses during handoff. To support these users, more neighboring APs should be pre-authenticated. To consider the user's service level, we defined the weight bound value according to the users' service class. According to the value, the number of selected APs for each user is limited.

Using Eq. (1) and (2), we can obtain an N by N weight matrix, *W*. N denotes the number of APs. *W* represents the weighted bi-directional graph of AP placements. Using the *W*, the identifier of current AP, and a weight bound value, the FHR for a user can be selected. Detailed procedure is presented in [6]. The procedure is similar to that of Dijkstra's algorithm.

3.2 Modified Key Distribution in IEEE 802.1x Model

Since IEEE 802.1x supports only one to one message delivery, the modified key distribution is required. Fig. 3 and 4 show the proposed key distribution. The one-time password scheme is used for the user authentication. Although a mobile host sends an authentication request to the AAA server, the server sends multiple authentication responses to all APs within an FHR. After receiving responses, APs except the current AP keep the authenticated information during a specific time period (*soft state*). If there is no handoff event during that period, the information expires and the mobile host should perform re-authentication when a handoff event occurs. In the Diameter protocol, the valid time period value of a session is delivered using an Attribute Value Pair (AVP) [4]. In addition, multiple keys can be distributed to the mobile host using multiple AVPs.

Fig. 4 shows the re-authentication message flow after handoff events. We assumed the AP(B) is an AP belonging to the FHR. If a mobile host hands off to AP(B), since the AP(B) receives session information in advance, further message exchanges are not needed. In 802.1x model, the controlled port changes into the authorized state after authentication procedures. In our scheme, since ports are in the ready state for fast handoff after receiving a grant response message from the AAA server, the port in the ready state can be changed into the authorized state just by checking the identifier of the mobile host, without further interaction with the AAA server. Therefore, the total handoff latency can be decreased.

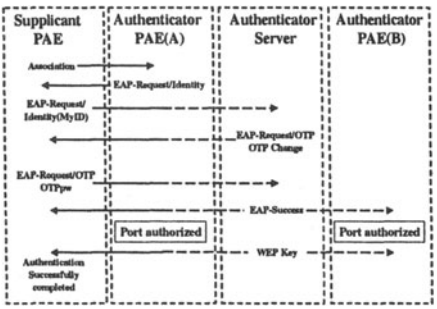

Fig. 3. Message Flow before Handoff

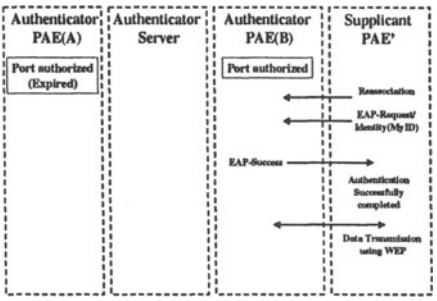

Fig. 4. Message Flow after Handoff

4. PERFORMANCE EVALUATION

4.1 Simulation Environment

For the performance evaluation, we assumed a simulation environment in Fig. 5. In this environment, AP(4) is the current AP of a mobile host. In this simulation, we assumed that there are three types of services: Class 1, 2, and 3. Each class has three weight bound values, 1, 2, and, 3, respectively. User *i* denotes a user in the class *i*.

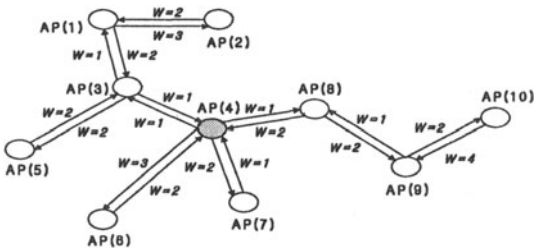

Fig. 5. Simulation Environment

We used the independent and identically distributed (*i.i.d.*) mobility model [5]. In this model, time is slotted and a mobile host can make at most one move during a slot. If a host is in AP(*i*) at the beginning of a slot, then during the slot it moves to AP(*i*+1) with probability *p*, moves to AP(*i*–1) with probability *q*, or remains in AP(*i*) with probability 1-*p*-*q*, independently of its movements in other slots. Each transition probability can be found based on Eq. (2). To consider the weight value of stable hosts, we used the stability factor, α. If $\alpha = 0$, the mobile host hands off to another AP with probability

1. On the other hand, if $\alpha = \infty$, the mobile host stays in the current AP. Eq. (3) shows the transition probability between APs. $P(i, j)$ is the transition probability from AP(i) to AP(j) and G is the normalization constant.

$$P(i,j) = \begin{cases} \frac{1}{G} \cdot \frac{1}{w(i,j)} & (i \neq j) \\ \frac{1}{G} \cdot \alpha & (i = j) \end{cases} \quad \left(G = \sum_{j \neq i} \frac{1}{w(i,j)} + \alpha \right) \tag{3}$$

4.2 Result & Analysis

In this section, we compare the handoff latency in the proposed fast handoff scheme, the preauthentication scheme, and the general handoff scheme. The total latency is the summation of the latencies in both the wireless network and the wired network. Each latency is proportional to the hop delay in each link and the number of message exchanges. We didn't consider any processing time in the AAA server.

Fig. 7 shows the average latency when the AAA server is located in the local domain. According to the *FHRSelect* algorithm [6], user 1 with the lowest priority authenticates only three APs. On the other hand, user 2 and 3 authenticate five and eight APs, respectively. The handoff latency of the proposed scheme is about a half of that of the general scheme. The latency of the preauthentication scheme is similar to that of class 2. However, it requires more network resources. Fig. 8 shows the result in case of the remote AAA server. We found that the average latency in this case is much higher than that of the local sever in the general scheme. However, the latencies in the proposed scheme remain same. This is because the handoff is completed by message flows only in the wireless link. There are no re-authentication message deliveries and further server processing.

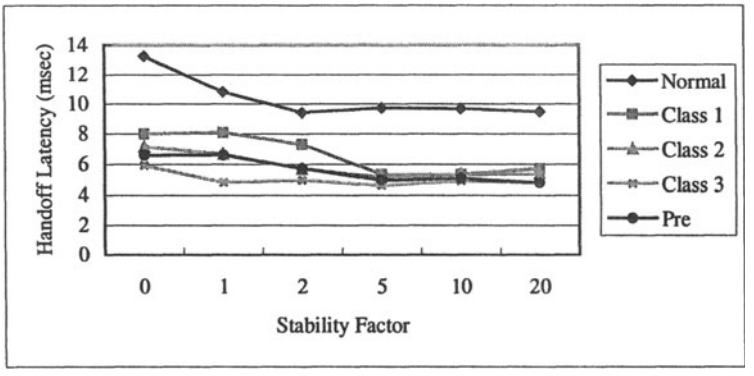

Fig.7. Average Handoff Delay (Local AAA Server)

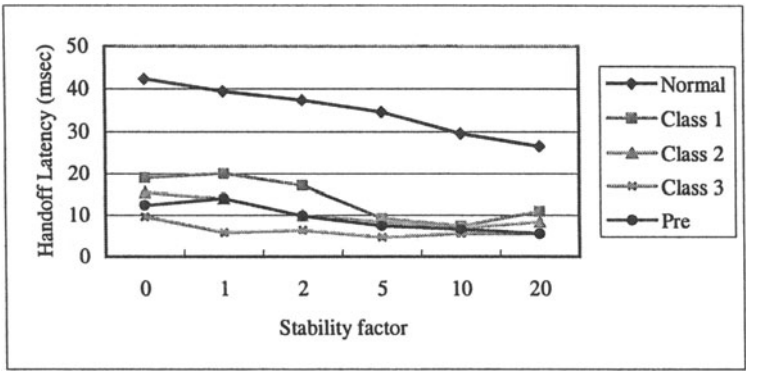

Fig.8. Average Handoff Delay (Remote AAA Server)

5. CONCLUSION

In this paper, we proposed a fast handoff scheme for a public wireless LAN system. Since the handoff and re-authentication procedures are essential in public wireless LAN, we focused on the minimization of the authentication latency during the handoff. In our scheme, multiple APs selected by the predictive algorithm. The algorithm utilizes traffic patterns and users' characteristics, which are collected and managed in the centralized system. Simulation results show that the total handoff latency of the proposed scheme is much less than that of the general handoff scheme and the preauthentication scheme. In the case where the AAA server is located in a remote domain, there is an even greater decrease in handoff latency.

REFERENCE

1. IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1x-2001, June 2001.
2. A. T. Campbell and J. Gomez, "IP Micro-Mobility Protocols," ACM Mobile Computing and Communication Review, Oct. 2000.
3. Matthew S. Gast, "802.11 Wireless Networks -The Definitive Guide," O'Reilly, 1st Edition, April 2002.
4. Pat R. Calhoun et al., "Diameter Base Protocol," Internet draft, draft-ietf-aaa-diameter-10.txt, April 2002.
5. A. Bar-Noy, I. Kessler, and M. Sidi, "Mobile Users: To Update or Not to Update?" ACM/Baltzer Journal of Wireless Networks, July 1995.
6. Sangheon Pack and Yanghee Choi, "Fast Inter-AP Handoff using Predictive-Authentication Scheme in a Public Wireless LAN," Networks 2002 (Joint ICN 2002 and ICWLHN 2002), Aug. 2002.