INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS
Int. J. Commun. Syst. 2007; **20**:515–531
Published online 9 August 2006 in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/dac.831

Evaluation of authentication interworking methods among multiple WLAN service providers

Wan Yeon Lee[1,*,†] and Heejo Lee[2,‡]

[1] *Department of Computer Engineering, Hallym University, Chunchon 200-702, South Korea*
[2] *Department of Computer Science and Engineering, Korea University, Seoul 136-713, South Korea*

SUMMARY

The interworking technologies to combine multiple WLANs into a single virtual system have not been studied extensively, particularly for legacy wireless networks. In this paper, we study how to provide the inter-domain authentication among multiple WLAN service providers with minimum overhead. We introduce five inter-domain authentication methods, referred to as *Info-Sharing*, *AP-Seq*, *AP-Con*, *AS-Seq* and *AS-Con*, which are designed in the form of an extension to the standard IEEE 802.1x and EAP protocols. In order to evaluate these methods, we compare their authentication time, implementation cost, confidentiality, flexibility and increment of messages. From the evaluation with analysis and experiments, we show that the *AS-Con* method can provide the authentication interworking function with minimal overhead on legacy network equipments. Also it is shown that, even though the authentication of *AS-Con* takes longer than the previous method, their difference is under one second and insensitive to users. Copyright © 2006 John Wiley & Sons, Ltd.

Received 1 August 2005; Revised 1 March 2006; Accepted 1 May 2006

KEY WORDS: wireless LAN; authentication; interworking; legacy network; 802.1x; EAP

1. INTRODUCTION

Wireless LAN (WLAN) technologies, particularly the IEEE 802.11 standard [1], have received a great deal of attention in recent years [2]. WLAN's access points (AP) are not only installed in corporate environments as a convenient extension to the wired LANs, but are starting to be deployed in public hot spots, such as airports, hotels and Internet cafes, as a means of providing

*Correspondence to: Wan Yeon Lee, Hallym University, Chunchon 200-702, South Korea.
† E-mail: wanlee@hallym.ac.kr
‡ E-mail: heejo@korea.ac.kr

Contract/grant sponsor: Institute of Information Technology Assessment; contract/grant number: B1220-0401-0188
Contract/grant sponsor: Korea Ministry of Information & Communications

public Internet access. Commercial services offering public Internet access are widely available on the market [3] and mobile users can get fast and reliable Internet access through these hot spots by using their own laptop computers or mobile devices.

In a commercial WLAN system, a mobile user needs to subscribe one service by paying the required fee and thereby obtaining the privilege to access public wireless networks. However, in this case, the services are only available in the areas where the service provider has already installed its APs. To extend the service areas, the service provider must deploy more APs, which implies additional costs. In order to extend the service areas without purchasing additional equipments, it can be considered that a service provider gives its subscribers the network access of other service providers. By sharing network equipments among different service providers, each provider can reduce the cost of deploying APs and increase the availability of the service offered. However, the interworking technologies to share legacy networking equipments between network domains have not been studied extensively. In this paper, we investigate the interworking technology of the authentication procedure among multiple WLAN service providers, in order to allow a subscriber to use the network infrastructure of other WLAN service providers.

Most previous works focused on studying the methods allowing for the fast handoff or secure authentication within a single WLAN system [4–7]. Some interworking methods have been studied for the interworking between two WLANs [8–11] and for the interworking between WLAN and CDMA2000 [12, 13]. However, these methods did not consider how to combine the network infrastructure of multiple service providers into a single virtual system. Moreover, it has not been evaluated which method is the most suitable for interworking multiple WLANs with minimum overhead, especially for legacy systems. Furthermore, their strength and weakness when they are applied to the interworking of multiple legacy WLAN systems have not been examined. RFC2865 [8] and RFC3588 [9] studied the interworking method between two authentication servers but did not consider how to efficiently interwork multiple WLANs belonging to different service providers. Iyer [10] proposed a new architecture to combine multiple WLANs into a single virtual system. But, this new common platform is designed for the future WLAN system and thus it would require a lot of modifications if it were applied to legacy WLAN systems. Buddhikot *et al.* [12] and Saleh [13] investigated Mobile IP-based interworking architectures providing integrated service capability across the 3G CDMA2000 and the 802.11 networks. These two studies considered the interworking method only within a single service provider but not among multiple service providers.

To support the authentication interworking function among multiple WLAN service providers, we introduce five inter-domain authentication methods described as follows:

- *Info-Sharing method*: each authentication server (AS) additionally manages the information of the subscribers pertaining to other WLAN systems.
- *AP-Seq method*: each AP performs an additional authentication sequentially in conjunction with one of the ASs in the other WLAN systems until this authentication is successfully completed.
- *AP-Con method*: each AP performs an additional authentication concurrently in conjunction with all of the ASs in the other WLAN systems.
- *AS-Seq method*: each AS performs an additional authentication sequentially in conjunction with one of the ASs in the other WLAN systems until this authentication is successfully completed.

DOI: 10.1002/dac

- *AS-Con method*: each AS performs an additional authentication concurrently in conjunction with all of the ASs in the other WLAN systems.

These methods are designed in the form of an extension to the standard IEEE 802.1x and EAP protocols. We first design these methods on the basis of the 802.1x [14] and EAP-MD5 [15, 16] protocols, because they are prevalently used in commercial legacy WLAN markets. Next, we attempt to apply these methods to other protocols such as EAP-TLS [17], EAP-TTLS and PEAP [15]. Due to the vulnerable security of these EAP protocols, RFC4017 [18] and 802.11i protocol [19] are being developed as an alternative of these EAP protocols. However, because these EAP protocols have been widely deployed in commercial systems, the interworking technology of legacy WLANs should be studied on the basis of these protocols.

It is important particularly for commercial legacy systems that the authentication interworking function should be implemented with minimum overhead. Thus, in this paper, we evaluate their overhead when these five methods are implemented upon legacy WLAN systems, in terms of their authentication time, implementation cost, confidentiality of system, flexibility to network changes and increment of messages. Through analytical evaluation and practical experiments, we verify that the *AS-Con* method is the most suitable for interworking multiple legacy WLANs based on the 802.1x and EAP protocols. Also we show that its increased authentication time is insignificant for the users and service providers, because its increment is usually under one second in a commercial system and thereby its difference is insensitive to users.

This paper is organized as follows: In Section 2, we explain the previous authentication method in a single WLAN system. In Section 3, we define the problem and introduce five authentication interworking methods. In Section 4, we evaluate these five methods and verify which method is the most suitable for the interworking of legacy systems. Finally, we conclude this paper and discuss future works in Section 5.

2. PREVIOUS AUTHENTICATION

In this section, we describe the previous authentication procedures based on the 802.1x and EAP-MD5 protocols. The 802.1x protocol defines the port-based network access control mechanism which authenticates and authorizes a mobile device to utilize a LAN port [14]. Figure 1 describes the flow of the message frames among the mobile terminal (MT), AP and AS in the 802.1x and EAP-MD5 protocol, where the number associated with each message denotes the sequence of that message among the multiple messages exchanged. The AP is responsible for relaying the frames between the MT and the AS. The sequence of operations of the 802.1x protocol is as follows: The MT initiates the authentication sequence by sending the EAPOL-Start frame and receiving the EAP-Request frame to request the information associated with the mobile user. The MT sends the ID information of the mobile user to the AS along with the EAP-Response and the Radius–Access–Request frame. Then, the AS sends an authentication query to the MT along with the Radius–Access–Challenge and the EAP-Request frame. To respond with an answer to this query, the MT transmits the EAP-Response and the Radius–Access–Request frame. Finally, after authorizing the answer, the AS sends the

DOI: 10.1002/dac

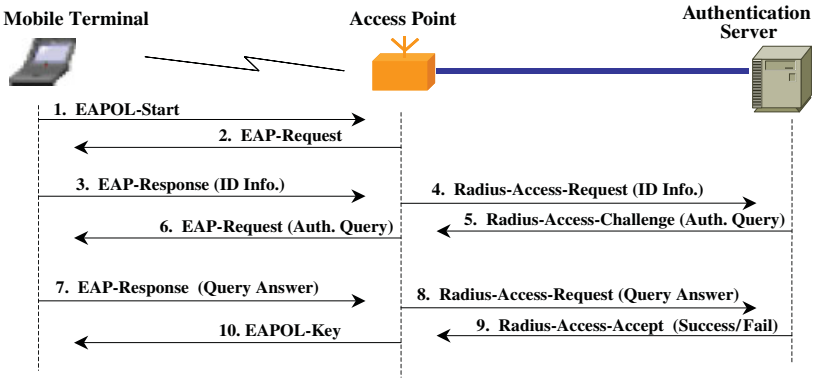

Figure 1. The flow of message frames in the 802.1x and EAP-MD5 protocol.

acceptance or rejection of this authentication procedure to the AP along with the Radius–Access–Accept frame.

Extensible Authentication Protocol (EAP) defines the means of communicating the authentication information between the AP and AS [15]. The EAP protocol actually confirms whether a user is authorized or not. EAP is a general protocol that supports a number of different authentication schemes, including EAP-MD5, EAP-TLS, EAP-TTLS and PEAP. In EAP-MD5, the User ID is used for the ID information and the password is used for the additional authentication query. The encapsulated format of EAP, known as EAP over LANs (EAPOL), is used for the communication between the MT and the AP, and the Radius protocol [20] is used for the communication between the AP and the AS. The detailed format of the Radius messages is shown in Figure 2. In the Radius protocol, a Secret Key is defined for the secure communication between the AP and the AS, and it is confidentially managed only in the AP and the AS. Request Authenticator field contains a randomly generated 16-bit value. The EAP-Authenticator and the Response Authenticator fields store the hash results which are calculated as follows (+ is the concatenation operation of strings):

- EAP-Authenticator = HMAC-MD5 (Header + Request/Response Authenticator + Message Content + Secret Key);
- Response Authenticator = MD5 (Header + Request Authenticator + Message Content + Secret Key).

Whenever the AP and the AS communicate a message, both of them individually calculate the EAP-Authenticator value using the message content and the Secret Key. When sending a message, the AP or the AS calculates the EAP-Authenticator field and attaches it to the message. Then, when receiving the message, the AP or the AS checks whether the attached EAP-Authenticator value is equal to the value calculated by itself. Also, the AP sends a randomly generated value in the Request Authenticator field whenever it sends the User ID or the answer to the authentication query to the AS (the Radius–Access–Request frame). Both the AP and the AS calculate the Response Authenticator value using the randomly generated value and the Secret Key as the input values. Whenever the AP receives a frame from the AS (the Radius–

DOI: 10.1002/dac

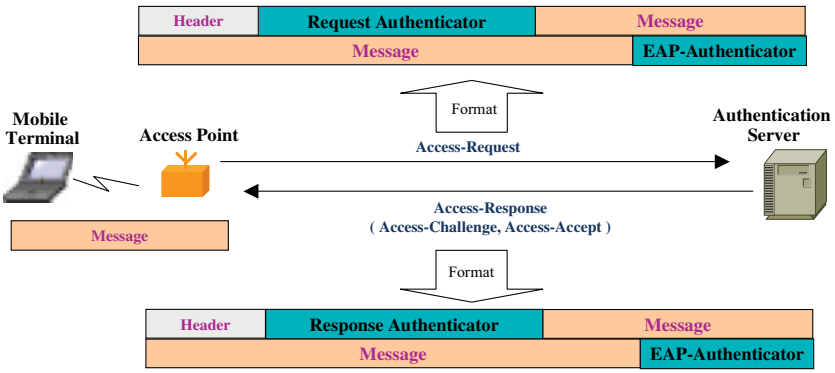

Figure 2. Radius message format.

Access–Challenge frame or the Radius–Access–Accept frame), it compares the transferred Response Authenticator and the Response Authenticator calculated by itself. The AP or the AS accepts a message only if the transferred EAP-Authenticator and the Response Authenticator values are equal to the corresponding values calculated by itself. As a result, only those network nodes knowing the Secret Key value can send or receive message frames during the authentication procedure.

3. AUTHENTICATION INTERWORKING

3.1. Problem definition

The authentication mechanism described in Section 2 does not allow a user to successfully complete the authentication procedure, if the user is located in the coverage areas of another WLAN service provider to which the user is not subscribed. Then the user must use the communication service offered by the other service provider, because the user's own service provider does not offer the communication service in these areas. Figure 3 shows an example in which a mobile user subscribed to Provider A moves into areas of Provider B. Since the communication service of Provider A is not available in the coverage areas of Provider B, the user must utilize the communication service of Provider B after being authenticated through the network of Provider B. To accomplish this, it is necessary to develop an authentication method which enables a mobile user to use the network of another service provider through a valid authentication procedure. We refer to this method as the *inter-domain authentication* method, and define the network infrastructure of a given WLAN service provider as the WLAN *domain*. In this paper, we consider only the interworking of legacy WLAN systems. Thus the inter-domain authentication needs to be implemented with minimal modification upon legacy systems, because these systems are already deployed and used in the commercial markets.

We assume that there are M service providers and all of them have agreed to share their networks with one another. It is also assumed that each mobile user subscribes to only one service provider. We define several new terminologies to explain the inter-domain authentication

DOI: 10.1002/dac

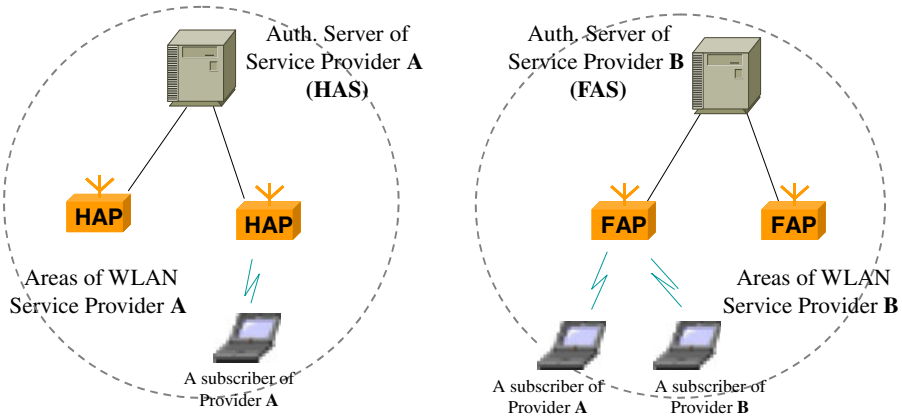

Figure 3. An example of sharing networks between two WLAN domains.

methods. The authentication server of the service provider to which the mobile user subscribed is defined as the Home Authentication Server (HAS), the access point of the service provider to which the mobile user subscribed is defined as the Home Access Point (HAP), the authentication servers of the other service providers are defined as the Foreign Authentication Servers (FASs), and the access points of the other service providers are defined as the Foreign Access Points (FAPs).

3.2. Inter-domain authentication methods

In this section, we introduce five inter-domain authentication methods. A simple method of providing inter-domain authentication is for each WLAN domain to maintain the information for all subscribers of other WLAN domains as well as that of its own WLAN domain. We call this the *Info-Sharing* method. The Info-Sharing method is easy to be implemented technically, however, there are several problems concerning the maintenance of up-to-date subscriber information and the management of accounts and billing data. Moreover, in cases where the disclosure of the information for the subscribers of one provider to another provider is not permissible, this approach is inappropriate for the inter-domain authentication.

The second approach is *AP-based*, which works without revealing the subscriber's information to other providers. In this method, each AP plays a key role, by acting as an interworking agent for the remote authentication, such as shown in Figure 4. When a subscriber moves into the coverage areas of another WLAN domain and initiates an authentication procedure, the AP of the other WLAN domain carries out the authentication procedure in conjunction with the AS managing the subscriber's information. When the AP recognizes that the authenticating procedure and its AS is failed, it next tries the authentication procedure in conjunction with the other ASs in the partner domains. Figure 4(a) shows the case that the AP tries the authentication procedure one by one sequentially with one of ASs in the partner domains until its authentication procedure succeeds, and we call it *AP-Seq*. Figure 4(b) shows the case that the AP concurrently tries the authentication procedure with all of the ASs in the

DOI: 10.1002/dac

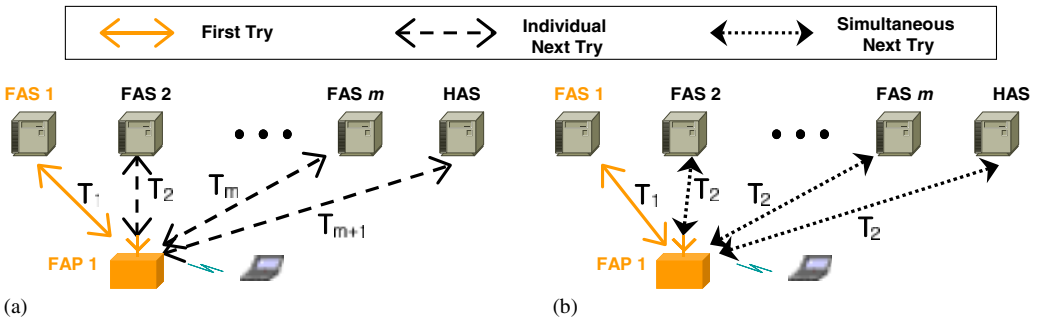

Figure 4. Using AP as the interworking agent for remote authentication: (a) serial next tries; and (b) concurrent next try.

partner domains and we call it *AP-Con*. In the AP-based approach, each AS manages the information concerning its own subscribers independently and, thus, the subscriber's information is not exposed to other service providers. The AP-based approach is formally described below.

3.2.1. AP-based approach

Step 1: Whenever the MT sends an authentication request message to the AP, the AP transfers it to the AS in its own domain.

Step 2: If the AP receives a message including an authentication query from the AS in its domain, the AP transfers it to the MT. Then, the AP transfers the reply message sent from the MT to the AS.

Step 3: If the AP receives the message of a failure notice from the AS, the AP relays the authentication request message sequentially (or concurrently) to all ASs in the other partner domains.

3.1: If the AP receives a message including an authentication query from an AS in another domain, the AP transfer it to the MT.

3.2: The AP relays the message sent from the MT to the AS in the other domain which sent the authentication query. Then, the AP relays the message sent from the AS in the other domain to the MT.

3.3: If the AP receives only the messages of a failure notice from all ASs of the other partner domains, the AP notifies the MT of the authentication failure.

Figure 5 shows the detailed message flow of this approach. The numbers adjacent to the arrows in this figure denote the sequence of the message frames in the IEEE 802.1x protocol. When a subscriber sends a request for authentication to an AP in the coverage areas of another WLAN domain (FAP), the AP first tries the authentication procedure associated with its AS (FAS) and, if this fails, it then tries the additional authentication procedure with the ASs of other systems. To implement *AP-Seq* or *AP-Con*, a new functionality needs to be added to each AP in all partner WLAN domains. The functionality is that each AP manages the addresses of ASs in the other partner domains in advance and attempts the next authentication process in conjunction with these ASs sequentially or concurrently if the first authentication process fails. We call this functionality *AP authentication function*. In addition,

DOI: 10.1002/dac

the Secret Key available only to the HAP and HAS for the secure communication should be open to the FASs, because the HAP also exchanges messages with the FASs during the additional authentication attempt.

The last approach is *AS-based*, in which the AS plays the role of the interworking agent for the process of remote authentication. When a subscriber moves into the coverage areas of another WLAN domain and initiates the authentication procedure, the AS of the other WLAN domain (FAS) carries out the authentication procedure in conjunction with the AS of the subscriber's WLAN domain (HAS). When the AS recognizes that the authenticating procedure fails, it tries the additional authentication procedure in conjunction with the other ASs in the partner domains. Figure 6(a) shows the case that the AS tries the authentication procedure one by one sequentially with one of ASs in the partner domains until its authentication procedure succeeds, and we call it *AS-Seq*, which is identical to the previous proxy server [8, 9]. Figure 6(b) shows the case that the AS concurrently tries the authentication procedure with all of the ASs in the partner domains and we call it *AS-Con*. In

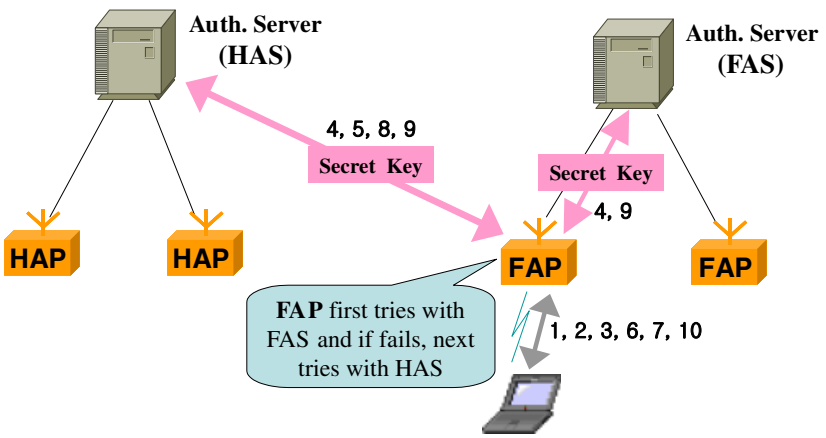

Figure 5. The message flow of the AP-based approach between two domains.

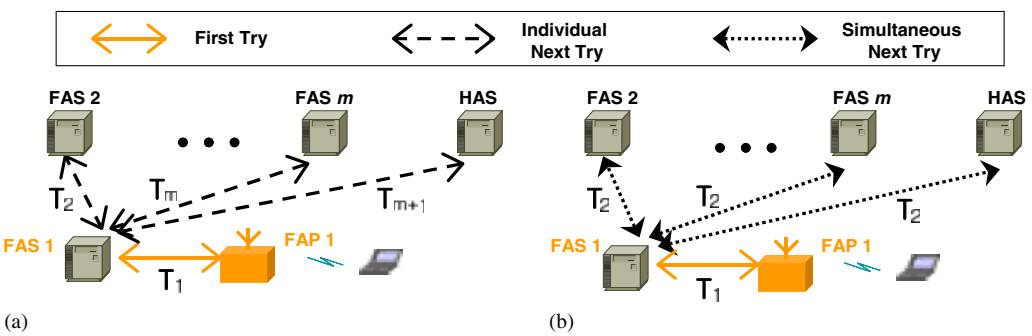

Figure 6. Using AS as the interworking agent for remote authentication: (a) serial next tries; and (b) concurrent next try.

DOI: 10.1002/dac

the AS-based approach, the FAS is responsible for relaying messages between the MT and the HAS. When relaying message frames, the FAS performs the repackaging of the message frames required to convert the EAP-Authenticator field and the Response Authenticator field defined for the communication between the FAP and the FAS into those defined for the communication between the FAS and the HAS. When converting the values of the EAP-Authenticator and the Response Authenticator, the Secret Key defined for the communication between the FAS and the HAS is managed independently of the Secret Key defined for the communication between the FAS and the FAP. We refer to the Secret Key used for the communication between the FAS and the FAP as the *Private* Secret Key, and the Secret Key used for the communication between the FAS and the HAS as the *Shared* Secret Key. The AS-based approach is formally described below.

3.2.2. AS-based approach

Step 1: Whenever the MT sends an authentication request message including the user ID to the AP, the AP transfers it to the AS in its own domain.

Step 2: The AS checks whether the received ID belongs to its subscribers. If the ID corresponds to one of its subscribers, the AS sends the authentication query to the AP.

Step 3: When the user ID does not belong to its subscribers, the AS relays the authentication request to all ASs in the other partner domains.

3.1: If the AS receives a message including an authentication query from an AS in another domain, the AS transfer it to the AP.

3.2: If the AS receives only the messages of a failure notice from all other ASs, the AS notifies the AP of the authentication failure.

Step 4: The AP transfers the message sent from the AS to the MT and the message sent from the MT to the AS.

Figure 7 shows the detailed message flow of the AS-based approach. The numbers adjacent to the arrows in this figure denote the sequence numbers of the corresponding message frames in

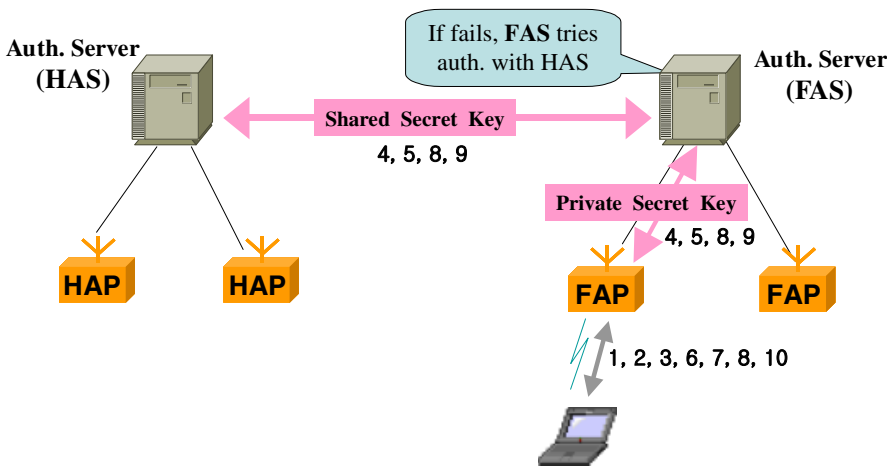

Figure 7. The message flow of the AS-based approach between two domains.

DOI: 10.1002/dac

the 802.1x protocol. When a subscriber initiates the authentication procedure in the coverage areas of another WLAN domain, the FAP tries the first authentication process with the FAS. If the FAS recognizes that the first authentication process has failed, it then tries the additional authentication process in conjunction with the HAS sequentially or concurrently. During this additional authentication process, the AS converts the EAP-Authenticator and the Response Authenticator fields of the message frames generated using the Shared Secret Key (or Private Secret Key) into those generated using the Private Secret Key (or Shared Secret Key). In these methods, therefore, it is not necessary to reveal the Secret Key to the ASs of the other WLAN domains. To implement *AS-Seq* or *AS-Con*, a new functionality needs to be added to each AS in all of the other WLAN domains. The functionality, called *AS authentication function*, is to manage the addresses of ASs in the other WLAN domains in advance and to carry out the additional authentication process.

4. EVALUATION

In this section, we evaluate the strengths and weaknesses of the five methods and verify which one is the most suitable for interworking multiple legacy WLAN systems. The evaluation is conducted in terms of their authentication time, implementation cost, confidentiality of the subscriber's information, confidentiality of the Secret Key, flexibility to changes of the interworking structure, and increment of messages.

4.1. Authentication time

We analyse the authentication time required for the communication of the ten message frames of the 802.1x protocol, described in Figure 1. In this analysis, we assume that no message is disappeared during its transmission and some of ASs may not reply to an authentication request due to changes of their operation environments; for example, they do not agree any more to share their networks with one another. We consider only the lower time bound and the upper time bound of successful authentications, because those of failed authentication are less meaningful. The communication time required to transmit the kth frame from the AP to its AS in the same domain is defined as t_k, the communication time required to transmit the kth frame from the AP to other AS in a different domain is defined as t'_k, and the communication time required to transmit the kth frame between two ASs is defined as t''_k. Then, the message flow of the Info-Sharing method is the same as that of the previous method. We refer to the lower bound and the upper bound of authentication times in Info-Sharing as $T_{\text{in}}^{\text{low}}$ and $T_{\text{in}}^{\text{up}}$, respectively. Then their values are

$$T_{\text{in}}^{\text{low}} = T_{\text{in}}^{\text{up}} = t_1 + t_2 + t_3 + t_4 + t_5 + t_6 + t_7 + t_8 + t_9 + t_{10}$$

The authentication times of the AP-based approach may be longer than that of the previous method, due to the additional authentication attempts. We refer to the lower bound and the upper bound of authentication times in AP-Seq as $T_{\text{ap}(s)}^{\text{low}}$ and $T_{\text{ap}(s)}^{\text{up}}$, respectively. Then their values are

$$T_{\text{ap}(s)}^{\text{low}} = t_1 + t_2 + t_3 + t_4 + t_9 + (m-1)\cdot(t'_4 + t'_9) + t'_4 + t'_5 + t_6 + t_7 + t'_8 + t'_9 + t_{10}$$

$$T_{\text{ap}(s)}^{\text{up}} = t_1 + t_2 + t_3 + (M-1)\cdot R\cdot\tau_o + t'_4 + t'_5 + t_6 + t_7 + t'_8 + t'_9 + t_{10}$$

DOI: 10.1002/dac

where AP completed successfully the additional authentication after receiving the rejection message sequentially from m ASs, and R is the number of retries to send again the authentication request to the same AS after the time period τ_o if any response message does not arrive. $T^{\text{low}}_{\text{ap}(s)}$ is the time when AP completes the authentication process successfully after receiving the rejection messages sequentially from its AS in its domain and $(m-1)$ ASs in other domains. $T^{\text{up}}_{\text{ap}(s)}$ is the time when AP completes the authentication process successfully with the last AS after not receiving any response message for the time $R \cdot \tau_o$ from the other $(M-1)$ ASs. We also refer to the lower bound and the upper bound of authentication times in AP-Con as $T^{\text{low}}_{\text{ap}(c)}$ and $T^{\text{up}}_{\text{ap}(c)}$, respectively. Then their values are

$$T^{\text{low}}_{\text{ap}(c)} = t_1 + t_2 + t_3 + t_4 + t_9 + t'_4 + t'_5 + t_6 + t_7 + t'_8 + t'_9 + t_{10}$$

$$T^{\text{up}}_{\text{ap}(c)} = t_1 + t_2 + t_3 + R \cdot \tau_o + t'_4 + t'_5 + t_6 + t_7 + t'_8 + t'_9 + t_{10}$$

$T^{\text{low}}_{\text{ap}(c)}$ is the time when AP completes the authentication process successfully with one of $(M-1)$ ASs after receiving the rejection message from its AS. $T^{\text{up}}_{\text{ap}(c)}$ is the time when AP completes the authentication process successfully after not receiving any response message for the time $R \cdot \tau_o$ from its AS.

Similarly, the authentication times of the AS-based approach may be longer than that of the previous method. We refer to the lower bound and the upper bound of authentication times in AS-Seq as $T^{\text{low}}_{\text{as}(s)}$ and $T^{\text{up}}_{\text{as}(s)}$, respectively. Then their values are

$$T^{\text{low}}_{\text{as}(s)} = t_1 + t_2 + t_3 + t_4 + (m-1) \cdot (t''_4 + t''_9) + t''_4 + t_5 + t''_5 + t_6 + t_7 + t_8 + t''_8 + t_9 + t''_9 + t_{10}$$

$$T^{\text{up}}_{\text{as}(s)} = t_1 + t_2 + t_3 + t_4 + (M-2) \cdot R \cdot \tau_o + t''_4 + t_5 + t''_5 + t_6 + t_7 + t_8 + t''_8 + t_9 + t''_9 + t_{10}$$

$T^{\text{low}}_{\text{as}(s)}$ is the time when AS completes the authentication process successfully after receiving the rejection messages from $(m-1)$ ASs in other domains. $T^{\text{up}}_{\text{as}(s)}$ is the time when AS completes the authentication process successfully with the last AS after not receiving any response message for the time $R \cdot \tau_o$ from the other $(M-2)$ ASs sequentially. We also refer to the lower bound and the upper bound of authentication times in AS-Con as $T^{\text{low}}_{\text{as}(c)}$ and $T^{\text{up}}_{\text{as}(c)}$, respectively. Then their values are

$$T^{\text{low}}_{\text{as}(c)} = T^{\text{up}}_{\text{as}(c)} = t_1 + t_2 + t_3 + (t_4 + t''_4) + (t_5 + t''_5) + t_6 + t_7 + (t_8 + t''_8) + (t_9 + t''_9) + t_{10}$$

$T^{\text{low}}_{\text{as}(c)}$ (or $T^{\text{up}}_{\text{as}(c)}$) is the time when AS completes the authentication process successfully with one of $(M-1)$ ASs in other domains after failing to complete this authentication process for itself.

Let us compare the lower bounds of their authentication times

$$T^{\text{low}}_{\text{ap}(s)} - T^{\text{low}}_{\text{in}} = (m-1) \cdot (t'_4 + t'_9) + (t'_4 + t'_5 + t'_8 + t'_9) - (t_5 + t_8)$$

$$T^{\text{low}}_{\text{ap}(c)} - T^{\text{low}}_{\text{in}} = (t'_4 + t'_5 + t'_8 + t'_9) - (t_5 + t_8)$$

$$T^{\text{low}}_{\text{as}(s)} - T^{\text{low}}_{\text{in}} = (m-1) \cdot (t''_4 + t''_9) + (t''_4 + t''_5 + t''_8 + t''_9) \quad \text{and}$$

$$T^{\text{low}}_{\text{as}(c)} - T^{\text{low}}_{\text{in}} = t''_4 + t''_5 + t''_8 + t''_9$$

This analysis implies that the lower bounds of authentication times in AP-Seq and in AP-Con are respectively about $m \cdot 20\%$ and about 20% longer than that in Info-Sharing, when t_k, t'_k, and t''_k are likely to be equal. Also, the lower bounds of authentication times in AS-Seq and in

DOI: 10.1002/dac

AS-Con are respectively about $(m+1)\cdot 20\%$ and about 40% longer than that in Info-Sharing. Also, let us compare the upper bounds of their authentication times

$$T^{\text{up}}_{\text{ap}(s)} - T^{\text{up}}_{\text{in}} = (M-1)\cdot R\cdot \tau_o + (t'_4 + t'_5 + t'_8 + t'_9) - (t_4 + t_5 + t_8 + t_9)$$

$$T^{\text{up}}_{\text{ap}(c)} - T^{\text{up}}_{\text{in}} = R\cdot \tau_o + (t'_4 + t'_5 + t'_8 + t'_9) - (t_4 + t_5 + t_8 + t_9)$$

$$T^{\text{up}}_{\text{as}(s)} - T^{\text{up}}_{\text{in}} = (M-2)\cdot R\cdot \tau_o + (t''_4 + t''_5 + t''_8 + t''_9) \quad \text{and}$$

$$T^{\text{up}}_{\text{as}(c)} - T^{\text{up}}_{\text{in}} = t''_4 + t''_5 + t''_8 + t''_9$$

This analysis implies that the upper bounds of authentication times in AP-Seq, AP-Con and AS-Seq heavily depend on the value of R or τ_o, because the available ranges of R and τ_o are from 1 to 10 and from 1 to 300 s, respectively [14]. On the contrary, the upper bound of authentication times in AS-Con is nearly equal to that in Info-Sharing, regardless of the value of M, R or τ_o.

To compare more precisely the authentication times, we examined the actual authentication times of these methods in practical systems. To examine the practical authentication times of AS-Seq and AS-Con, we implemented these two methods on a pentium PC with Redhat 9.0 Linux OS on the basis of 802.1x and EAP-MD5 protocols. The authentication times of Info-Sharing, AP-Seq and AP-Con are examined using one MT, one AP and two ASs, manufactured by the MMC Technology company. To estimate the authentication time of AP-Seq and AP-Con, we run the authentication procedure two times using the same MT and AP but different ASs. The first run is a failure case in conjunction with one AS (from the FAP to the FAS) and the second one is a success case in conjunction with the other AS (from the FAP to the HAS). We separately measured three values of $(t_1 + t_2 + t_3)$, $(t_4 + t_9)$ and t_{10} in the first run, and four values of $(t'_4 + t'_9)$, $(t'_4 + t'_5)$, $(t_6 + t_7)$, and $(t'_8 + t'_9)$ in the second run, using the Ethereal packet sniffing program. And we utilize these values to estimate the authentication times of AP-Seq and AP-Con. In these experiments, the AP (FAP) and one AS (FAS) directly connect to a hub, but the other AS (HAS) connects to the hub via various numbers of intermediate nodes. The examined values of the authentication times, which are the average values of 20 times runs.

Figure 8(a) shows the experimental values of the fastest authentication in AP-Seq and AS-Seq, and Figure 8(b) shows the experimental values of the fastest authentication in AP-Con and AS-Con. In this figure, *number of hops* refers to the distance (the number of intermediate nodes) between the FAP and the FAS (or the HAS). In Figure 8(a), the authentication times of AP-Seq and AS-Seq increase more rapidly as the value of m increases, while their authentication times slightly increases as the number of hops increases. In Figure 8(b), the authentication times of AP-Con and AS-Con slightly increase as the number of hops increases, while the authentication times of Info-Sharing are almost equal because its network configuration does not change.

Figure 9(a) shows the experimental values of the slowest authentication in AP-Seq and in AS-Seq, and Figure 9(b) shows the experimental values of the slowest authentication in AP-Con and in AS-Con. In this figure, W denotes the value of $R\cdot\tau_o$. In Figure 9(a), the authentication times of AP-Seq and AS-Seq increase very rapidly as the value of M increases, and the increment ratio becomes large as the value of W increases. In Figure 9(b), the authentication time of AP-Con is almost equal to the value of W and the authentication time of AS-Con is almost equal to that of Info-Sharing.

In these experiments, we observe that the increased authentication time of AS-Con is always insignificant for the users and service providers because the millisecond gaps are not crucial in current commercial systems. The increased authentication time of AP-Con is also negligible in

DOI: 10.1002/dac

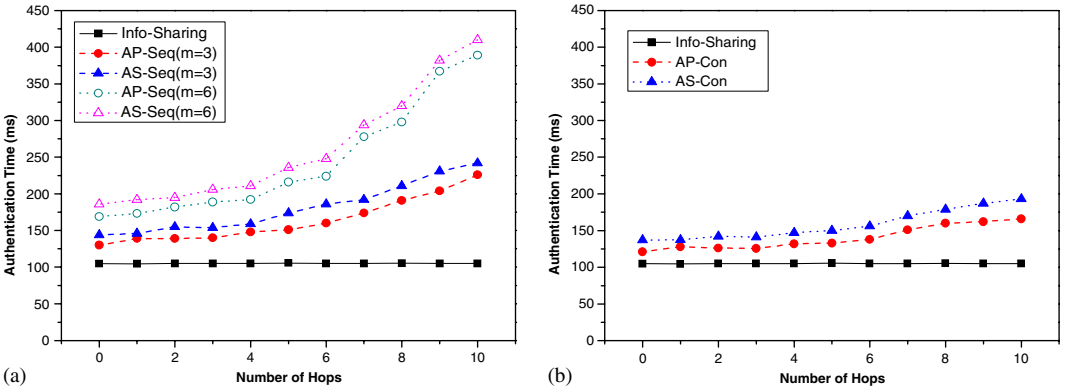

Figure 8. Comparisons of the smallest authentication time: (a) comparison of AP-Seq and AS-Seq with Info-Sharing; and (b) comparison of AP-Con and AS-Con with Info-Sharing.

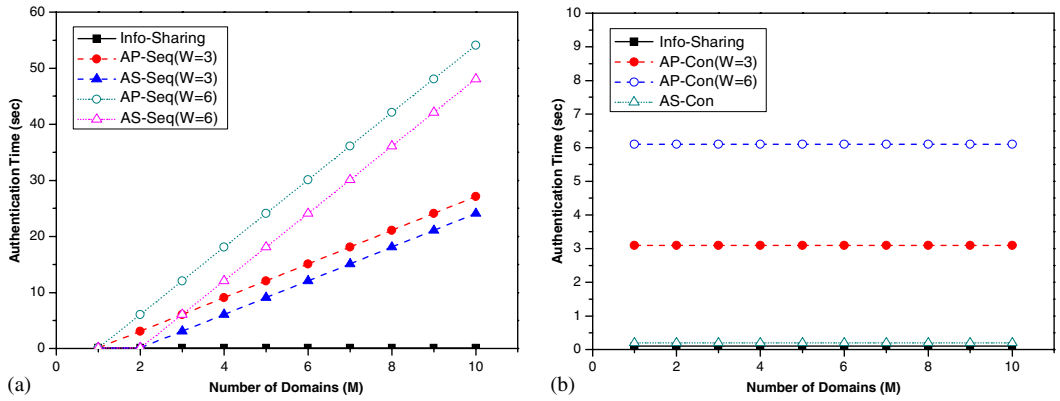

Figure 9. Comparisons of the largest authentication time: (a) comparison of AP-Seq and AS-Seq with Info-Sharing; and (b) comparison of AP-Con and AS-Con with Info-Sharing.

most cases except the worst case that AS does not reply to its AP in the same domain. On the contrary, the entire authentication times of AP-Seq and AS-Seq become significantly larger than that of the previous authentication method, if the value of m, M, or W becomes large. Thus it is possible that their increased authentication times are sensitive to users and make it inconvenient to use the WLAN service.

4.2. Implementation overhead

In addition to the authentication time, we also evaluate these methods in terms of their implementation cost, confidentiality, flexibility and increment of messages. *Cost* refers to the amount of S/W or H/W to be upgraded mandatorily in legacy WLAN equipments when implementing the given method. *Confidentiality* refers to whether or not the subscriber's information or the Secret Key is revealed to other partner WLAN domains. *Flexibility* refers to the cost of the modification required when adding, deleting or changing some of the partner

DOI: 10.1002/dac

WLAN domains which cooperate with one another in constructing a single virtual system. *Increment of messages* refers to the amount of increased messages when implementing the given method. The results of the evaluation are summarized in Table I.

To implement Info-Sharing, the information of the subscribers of the other WLAN domains needs to be inserted in the database of each AS. To implement AP-Seq or AP-Con, all of the APs need to acquire the new functionality of *AP authentication function* in order for them to attempt the additional authentication procedure in conjunction with the ASs in the other partner domains. Supplementing this new functionality to the legacy APs requires H/W upgrade because the authentication function of commercial APs is usually constructed with dedicated H/W modules. To implement AS-Seq or AS-Con, the AS needs to acquire the new functionality of *AS authentication function*, which allows it to attempt the additional authentication procedure in conjunction with the ASs in the other partner domains. This new functionality can be supplemented to the legacy AS only with S/W upgrade because the authentication function of commercial ASs is implemented in a S/W program.

We rate the confidentiality of Info-Sharing as low, because the subscriber's information has to be revealed to the other WLAN domains. The confidentiality of AP-Seq and AP-Con is rated as medium, because not the subscriber's information but the Secret Key has to be revealed to the ASs in the other partner domains. The confidentiality of AS-Seq and AS-Con is rated as high, because no confidential information needs to be revealed to the other partner domains. We rate the flexibility of Info-Sharing as low, because a large part of the subscriber's information in the database of each AS has to be modified whenever a partner domain is added, deleted or changed. The flexibility of AP-Seq and AP-Con is also rated as low, because the addresses with regard to the FAS in all APs have to be modified whenever a partner domain is added, deleted, or changed. In contrast, the flexibility of AS-Seq and AS-Con is rated as high, because the address of the FAS only in the S/W program of an AS needs to be modified whenever a partner domain is added, deleted or changed.

Info-Sharing does not require any additional message. In AP-Seq, AP additionally requires $2 \cdot m$ messages, where m is the number of ASs with which AP attempted but failed the additional authentication process before it completes successfully this process. In AP-Con, AP additionally requires $2 \cdot (M-1)$ messages for the concurrent authentication process with $(M-1)$ ASs. The average value of m is $\frac{(M-1)}{2}$ and thus the amounts of increased messages in AP-Seq and in AP-Con are $\frac{(M-1)}{2} \times 20\%$ and $(M-1) \times 20\%$, respectively. In AS-Seq, AS additionally requires $2 \cdot m$ messages for the sequential authentication and 4 messages for relaying between its AP and HAS. In AS-Con, AS additionally requires $2 \cdot (M-1)$ messages for the concurrent authentication and 4 messages for relaying between its AP and HAS. Thus the amounts of increased messages in AS-Seq and in AS-Con are $\frac{(M-1)}{2} \times 20 + 40\%$ and $(M-1) \times 20 + 40\%$, respectively.

Table I. Evaluation of implementation overhead.

Interworking methods	Costs	Confidentiality	Flexibility	Increment of messages
Info-Sharing	DB in one AS	Low	Low	0%
AP-Seq	HW in all APs	Medium	Low	$\frac{(M-1)}{2} \times 20\%$
AP-Con	HW in all APs	Medium	Low	$(M-1) \times 20\%$
AS-Seq	SW in one AS	High	High	$\frac{(M-1)}{2} \times 20 + 40\%$
AS-Con	SW in one AS	High	High	$(M-1) \times 20 + 40\%$

DOI: 10.1002/dac

4.3. Comparison

We compare the five methods, in order to determine which method is the most suitable for legacy systems based on the 802.1x and EAP-MD5 protocols. The increased authentication time in AP-Seq or in AS-Seq may incur a serious inconvenience to users, because its time is likely to be amplified as the value of M, R or τ_o increases. On the contrary, the increased amount of authentication times in AP-Con or in AS-Con may be insensitive to users in most cases. Consequently, AP-Con is better than AP-Seq and AS-Con is better than AS-Seq, even though the increased amounts of messages in AP-Con and in AS-Con are twice of those in AP-Seq and in AS-Seq, respectively. Thus we compare only the Info-Sharing, AP-Con and AS-Con methods.

Compared with AS-Con, Info-Sharing is impractical, because the subscriber's information has to be revealed to the other WLAN domains (low confidentiality) and a large part of the subscriber's information in the database of each AS needs to be modified whenever a partner WLAN domain is added, deleted or changed (low flexibility). Compared with AS-Con, AP-Con is also impractical, because a considerable number of APs need to replace their HW modules (high cost), the Secret Key is revealed to the AS of the other WLAN domains (medium confidentiality), and all of the APs in each domain need to be modified whenever a partner WLAN domain is added, deleted or changed (low flexibility). The increased authentication time or the increased amount of messages required for AS-Con is not critical when considering the other important features related to inter-domain authentication. Consequently, we can conclude that AS-Con is the best solution to the problem of supporting the authentication interworking functionality in multiple legacy WLAN systems with the minimum overhead.

In addition, we evaluate the extensibility of the five methods when they are applied to other common protocols such as EAP-TLS, EAP-TTLS and PEAP, instead of EAP-MD5. While the EAP-MD5 protocol only performs the user authentication at the server node, the EAP-TLS protocol performs the server authentication process at the user node before starting the user authentication process [17]. Similarly, the EAP-TTLS and PEAP protocols perform the user authentication process only after the successful completion of the server authentication process [15, 17]. In these protocols, the MT confirms that the AS with which it is communicating is the AS of its own domain (the server authentication process) before starting the authentication process for the user (the user authentication process) at the AS. Thus, Info-Sharing can be applied to the systems based on the EAP-TLS, EAP-TTLS, or PEAP protocols, because the server authentication process can be performed successfully if the certificate of the HAS is copied into the FAS. Also the AP-based methods can be used on these systems. If the server authentication process has failed at the user node (the MT), the MT notifies it to the AP. Thus, the FAP can detect this failure when the server authentication fails. If the FAP attempts the server authentication process in conjunction with the HAS when the FAP detects that the server authentication process with the FAS has failed, the server authentication process can be performed successfully. Similarly, the AS-based methods can be applied to these systems. If FAS forwards the packets corresponding to the server authentication process to HAS or FAP, the server authentication of HAS instead of that of FAS can be successfully performed at the user node. Their implementation overhead when they are applied to EAP-TLS, EAP-TTLS, or PEAP protocol-based systems is almost equal to that when they are applied to EAP-MD5 protocol-based systems, described in Table I. Furthermore, the increased authentication times of AS-Con may be not sensitive to users by the reason explained in Section 4.1. Consequently,

DOI: 10.1002/dac

we can conclude that AS-Con is also the most suitable for the interworking of legacy WLAN systems based on the EAP-TLS, EAP-TTLS, or PEAP protocols.

5. CONCLUSIONS

Inter-domain authentication allows one service provider to give network access to a subscriber of another service provider in order to attract more customers by increasing the coverage of public wireless access. To do so, an authentication interworking method is required, which allows a subscriber to successfully complete the authentication procedure in the coverage areas of another WLAN domain. We introduced five inter-domain authentication methods and evaluated these methods in terms of their authentication time, implementation cost, confidentiality, flexibility and increment of messages. In the Info-Sharing method, each authentication server manages the information of all subscribers, including those belonging to the other WLAN domains. In the AP-Seq or AP-Con methods, the access point plays the role of the interworking agent for the remote authentication procedure sequentially or concurrently. In the AS-Seq or AS-Con methods, the authentication server plays the role of the interworking agent for the remote authentication procedure. From the extensive evaluation, it is verified that AS-Con is the most suitable for interworking multiple legacy WLAN systems based on the 802.1x and EAP protocols.

In this paper, we do not consider the seamless handoff operation [21] between APs belonging to different WLAN service providers. Thus, we will study the authentication interworking method to support an efficient handoff operation between different WLAN service providers. Also, we will study the interworking method of the billing procedure among multiple WLAN service providers.

ACKNOWLEDGEMENTS

This research was supported by the Institute of Information Technology Assessment through the Information & Communication Fundamental Technology Research Program, grant number: B1220-0401-0188 and was additionally supported by the ITRC program of the Korea Ministry of Information & Communications.

REFERENCES

1. IEEE 802.11. *Part 11*: *Wireless LAN Medium Access Control* (*MAC*) *and Physical Layer* (*PHY*) *Specifications*, 1999.
2. Keene I, Calvert J. *Public Wireless LAN Hot Spots*: *Worldwide Trends and Forecasts*. Gartner Dataquest, August 2002.
3. Choi Y, Paek J, Choi S, Lee GW, Lee J, Jung H. Enhancement of a WLAN-based internet service in Korea. *ACM Workshop on Wireless Mobile Application and Service on WLAN Hotspots*, San Diego, CA, U.S.A., September 2003; 36–45.
4. Pack S, Choi Y. Fast inter-AP handoff using predictive-authentication scheme in a public wireless LAN. *Proceedings of IEEE Networks 2002* (*Joint ICN 2002 and ICWLHN 2002*), Atlanta, U.S.A., August 2002.
5. Bargh MS, Hulsebosh B, Ertink H, Prasad AR, Schoo P, Wang H. Fast authentication methods for handovers between IEEE 802.11 wireless LANs. *ACM Workshop on Wireless Mobile Application and Service on WLAN Hotspots*, Philadelphia, PA, U.S.A., October 2004; 51–60.
6. Matsunaga Y, Merino AS, Suzuki T, Katz RH. Secure authentication system for public WLAN roaming. *ACM Workshop on Wireless Mobile Application and Service on WLAN Hotspots*, San Diego, CA, U.S.A., September 2003; 113–121.

DOI: 10.1002/dac

7. Zhang J, Li J, Weinstein S, Tu N. Virtual operator based AAA in wireless LAN hot spots with ad-hoc networking support. *ACM SIGMOBILE Mobile Computing and Communication Review* 2002; **6**(3):10–21.
8. Rigney C, Willens S, Rubens A, Simpson W. Remote authentication dial in user service (RADIUS). *IEEE RFC 2865*, June 2000.
9. Calhoun P, Loughney J, Guttman E, Zorn G, Arkko J. Diameter base protocol. *IEEE RFC 3588*, September 2003.
10. Iyer P, Lortz V, Tapper L, Chandler R, Gryder R. Public WLAN hotspot deployment and interworking. *Intel Technology Journal* 2003; **7**(3):9–20.
11. Lee WY. Authentication interworking methods between wireless LAN systems. *IASTED International Conference on Networks and Communication Systems*, Krabi, Thailand, April 2005; 255–260.
12. Buddhikot MM, Chandranmenon G, Han S, Lee YW, Miller S, Salgarelli L. Design and implementation of a WLAN/cdma2000 interworking architecture. *IEEE Communications Magazine* 2003; **41**(11):90–100.
13. Saleh A. Mobile IP performance and interworking architecture in 802.11 WLAN/CDMA2000 networks. *Second Annual Conference on Communication Networks and Services Research*, Frederiction, NB, Canada, May 2004; 75–79.
14. IEEE standard 802.1x. *IEEE Standards for Local and Metropolitan Area Networks—Port-Based Network Access Control*. IEEE Standard Association: Piscataway, NJ, U.S.A., June 2001.
15. Aboba B, Blunk L, Vollbrecht J, Carlson J, Levkowetz H. Extensible authentication protocol (EAP). *IEEE RFC 3748*, June 2004.
16. Rivest R. The MD5 message-digest algorithm. *IEEE RFC 1321*, April 1992.
17. Aboba B, Simon D. PPP EAP TLS authentication protocol. *IEEE RFC 2716*, October 1999.
18. Stanley D, Walker J, Aboba B. Extensible authentication protocol (EAP) method requirements for wireless LANs. *IEEE RFC 4017*, March 2005.
19. IEEE standard 802.11i/D4.1. Medium access control (MAC) security enhancements. *IEEE 802.11 WG*, July 2003.
20. Aboba B, Calhoun P. RADIUS (Remote Authentication Dial In User Service) support for extensible authentication protocol (EAP). *IEEE RFC 3579*, September 2003.
21. IEEE standard 802.11f/D5. Draft recommended practice for multi-vendor access point interoperability via an inter-access point protocol across distribution systems supporting IEEE 802.11 operation. *IEEE 802.11 WG*, January 2003.

AUTHORS' BIOGRAPHIES

Wan Yeon Lee received his BS, MS, and PhD degrees in computer science and engineering from Pohang University of Science and Technology in 1994, 1996 and 2000, respectively. He is currently an Assistant Professor in the Department of Computer Engineering, Hallym University, Chunchon, Korea. From 2000 to 2003, he was a research engineer in LG Electronics and worked for the standardization of Next Generation Mobile Network of 3GPP Group. His research interest includes mobile computing, embedded system, real-time system, computer security, and parallel computing.

Heejo Lee received his BS, MS, PhD in Computer Science and Engineering from Pohang University of Science and Technology (POSTECH), Korea in 1993, 1995 and 2000, respectively. Since 2004, he has been an assistant professor at the Department of Computer Science and Engineering, Korea University, Seoul, Korea. From 2001 to 2003, he was at Ahnlab, Inc. as Chief Technology Officer (CTO) and Director of Technology Planning Department. From 2000 to 2001, he was a Post Doctoral Research Associate at the Network Systems Lab of the Department of Computer Sciences, and at the Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University. His research interest includes computer and communication security, parallel scientific computing, and fault-tolerant computing.

DOI: 10.1002/dac