EURASIP Journal on
Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

A novel pre-authentication scheme based on fast channel switching in IEEE 802.11 WLANs

JaeJong Baek[1], SungHoon Seo[2], Fei Shi[1] and JooSeok Song[1*]

Abstract

In the case of a 3G-WLAN interworking architecture, handoff latency is mainly caused by the delays incurred when a mobile station (STA) transfers a current security context to the target access network or establishes connectivity to a new access point (AP). Existing handoff optimization schemes have mostly focused on reducing the scanning time which is to discover nearby access points. Even though the time taken by a mobile STA to authenticate the target APs contributes to the total handoff delay, the schemes to optimize the authentication time have not yet been fully investigated for providing seamless connectivity to mobile users performing handoff in WLANs. As a solution, pre-authentication, a technique performing the authentication of target APs before the completion of the handoff procedure, has attracted considerable attention to reduce the overall delay related with a handoff, which is performed within inter-subnet and/or inter-administrative domain levels. Therefore, in this article, we propose a novel pre-authentication scheme to minimize the handoff delay in 3G-WLAN interworking architecture. The proposed scheme pre-authenticates a new AP directly through a switched channel in a short period of time. Our evaluation shows that the proposed scheme outperforms the existing authentication schemes defined in the IEEE 802.11 standards in terms of authentication delay, signaling cost, and mobility rate. The proposed mechanism offers an additional advantage in that it is easy to implement and deploy by simply modifying the device driver modules of clients' WLAN interfaces.

1 Introduction

Recently, the interworking between 3G cellular networks and wireless local area networks (WLANs) has become a global trend in wireless communications because of the fact that these networks exhibit characteristics such as wide coverage and high data rates that mutually complement each other. According to the recent trends, several schemes have been proposed in [1-3], these schemes combine WLANs and cellular data networks to form integrated wireless data networks. The 3rd generation partnership project (3GPP) has recently published the specifications of a 3G-WLAN interworking architecture [4] and their interworking architecture can be simplified as shown in Figure 1. This architecture introduces horizontal handoff (HH) and vertical Handoff (VH) [5]. An HH occurs when a mobile station (STA) roams within a network that uses the same radio technology, whereas a VH occurs when the mobile STA moves between networks that uses different radio technologies. Handoffs (HOs) are further subdivided into link-layer (L2) HOs and internet protocol (IP)-layer (L3) HOs [5]. This article focuses on the authentication operation during an L2 HH within WLANs with a 3G-WLAN interworking architecture. In the 3GPP interworking architecture, it is mandatory to provide special authentication, authorization and accounting (AAA) servers on a 3G home network (HN), generally including the entities like WLAN access gateway (WAG), packet data gateway (PDG), home subscriber server (HSS), home location register (HCR), and HAAA as shown in Figure 1, for interworking with WLAN's AAA services. Thus, given this requirement, if the 3G HN is located far away from the mobile STA and if it is separated by multiple networks and proxy AAA servers, a long authentication and HO delay will be taken. However, it should be noted that to achieve seamless mobility in a 3G-WLAN interworking architecture, the HO delay must be as short as possible.

Generally, an HO delay is composed of an access point (AP) scanning delay [6], authentication delay, and

* Correspondence: jssong@emerald.yonsei.ac.kr
[1]Department of Computer Science, Yonsei University, Shinchon, Seoul, South Korea
Full list of author information is available at the end of the article

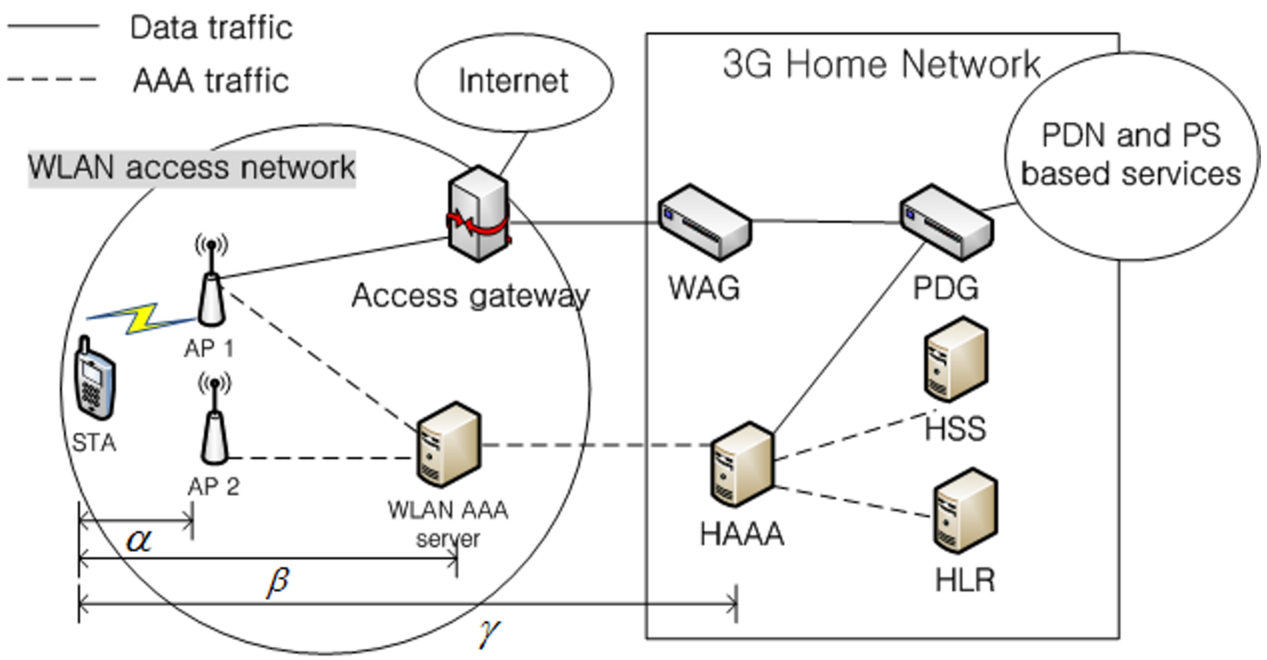

Figure 1 Simplified 3G-WLAN interworking architecture.

mobile IP registration delay in the case of an L3 HO [5]. AP scanning delay occurs in process when mobile STA searches for and selects a new AP. Authentication delay occurs in the process including establishing the identity of the mobile STA and authorizing its access to the basic service set of the AP. Mobile IP registration delay includes two kinds of delays. First one occurs in the HA registration process. Second one occurs when mobile STA configures a new network care of address in the foreign network. One of the main factors responsible for the HO delay has been reported to be the delay due to the authentication process between the WLAN and the 3G HN [5,7-9]. Existing HO optimization schemes primarily focus on reducing the delay caused when a mobile STA scans for nearby APs [10-14]. Even though the time taken by a mobile STA to authenticate the target AP (TAP) contributes to the total handoff delay, schemes to optimize the authentication time have not yet been fully investigated to mobile users performing handoff in WLANs. Therefore, we mainly focus on reducing the authentication delay using fast channel switching and a WLAN power saving mode (PSM) buffering function when the STA performs WLANs' HH in 3G-WLAN interworking. The advantages of the proposed scheme are summarized as follows: (a) the proposed scheme ensures a reduction in the authentication delay when a mobile STA moves from one AP to another; (b) it supports inter-extended service set (ESS) and inter-domain HOs without the need for modifying the currently deployed APs on the network side; (c) it prevents loss of data because it takes into account the buffering function of the APs; and (d) it overcomes the limitation of the radio coverage of the currently associated AP (CAP), which the existing authentication schemes suffer from when the moving STA perform authentication with the TAP.

The rest of the article is organized as follows. In Section 2, we provide the background of this study and describe previous related studies on pre-authentication in WLANs, using various protocols such as IEEE 802.11f, 802.11i, and 802.11r. Section 3 provides details of the proposed scheme, including the message flow and flow chart. In Section 4, we compare the performance of the proposed scheme with that of the conventional schemes and present the numerical results. We also analyze issues concerning the quality of service (QoS) and security. Finally, Section 5 presents the conclusions of this study.

2 Background and related works

To introduce our scheme, we will first briefly describe two basic operations, namely, channel switching operations and PSM operations. As in related studies, we will analyze three standard authentication solutions and one authentication solution that is under development.

2.1 Basic operations

2.1.1 Channel switching operations

A hotspot of WLAN is formed with at least one fixed length radio channel guided by physical standard of

IEEE 802.11. Figure 2 shows a scenario that a mobile STA tries to switch its radio channel to a better one within overlapped hotspots provided by a currently associated AP (CAP) and a TAP. Messages 1b and 2b in the scenario are to switch between two different channels provided by CAP and TAP. The time of channel switching generally takes 1 ms to 5 ms [11]. To authenticate with a TAP, a mobile STA must switch its channel to the communication channel configured at the TAP. When channel switching occurs, STAs suffer from two potential problems as follows: (1) in-transit packets at wireless links are missing which results the disruption in seamless services and (2) the service quality of in-use real-time applications at the STAs may degrade if channel is frequently switched. To prevent the first problem, we introduce a solution using PSM operations where details will be introduced in Section 2.1.2. Regarding the second problem, because pre-authentication is performed in a very short time with fast channel switching (FCS), STAs do not suffer from service degradation caused by the retransmission of lost frame and delayed ACK messages [14,15]. We conclude and make the definition of FCS as follows. The current IEEE 802.11 standard supports multiple channels. Our proposed scheme performed the pre-authentication with new channel by fast channel switching in a very short time. FCS is the method or operation for the mobile station to choose a different channel to listen to without losing the current channel session (data or packet).

2.1.2 Power saving mode operations (PSM)

In an infrastructure mode, an AP buffers every packet to be sent to the sleeping STAs to avoid frame loss, and notifies the buffer status through a traffic indication map (TIM) field in the beacon frame, which utilizes a shorthand method of listing association identifications (AIDs). As shown in Figure 2, each time the mode of the STA is changed, APs record the status of STAs (power saving mode or awake mode) and perform the function of buffering and forwarding. Power saving mode (PM) is a lower-power mode in which the interface cannot send or receive data. Awake mode (AM) is a higher power mode in which the interface allows data flow. It should be noted that a fake PSM message can be created and sent by adjusting the IEEE 802.11 frames (messages 1a and 2a shown in Figure 2). The fake PSM message is defined as follows. As shown in this figure, STAs only notify the AP to enter PM, however, the actual mode of the STAs is the AM. After a listen

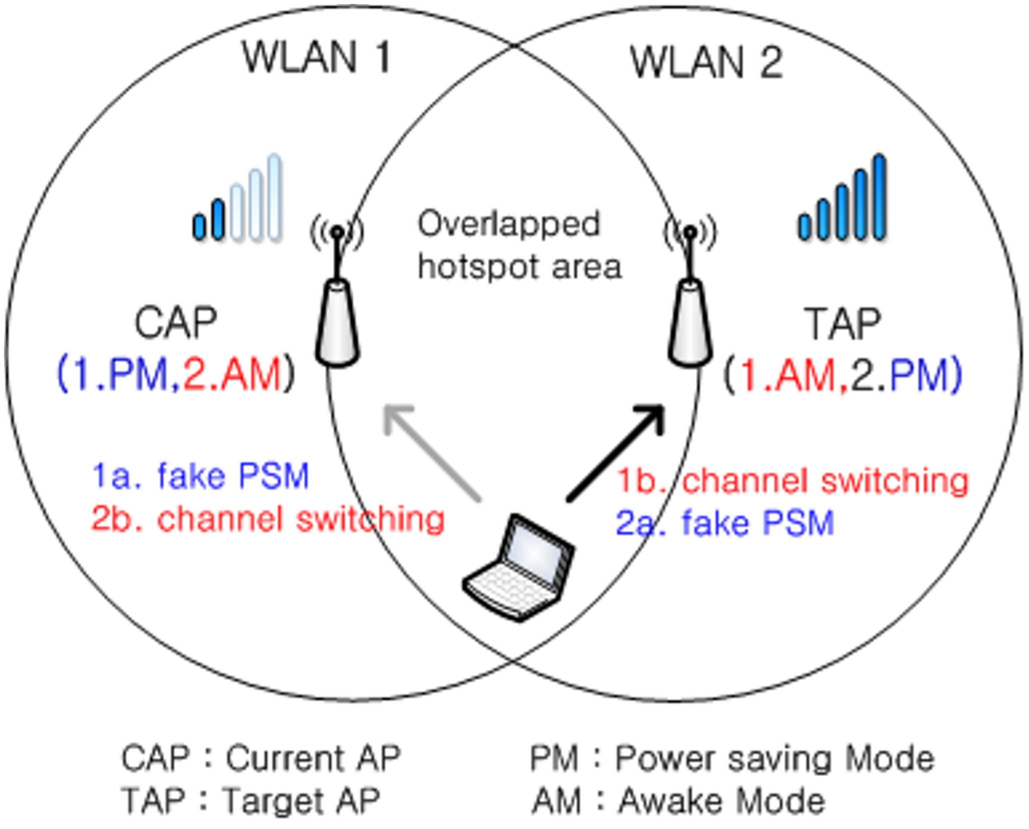

Figure 2 Concept of channel switching with PSM.

interval (LI), the STAs in PM have to periodically listen to and check for the beacon frame coming from the APs. As soon as an STA notifies the presence of a buffered frame for itself, it will send a power-save poll (PS-Poll) frame to the AP to retrieve the buffered frame. Otherwise, the STAs remain in the PM until the next beacon frame is transmitted [16].

2.2 Related works

2.2.1 Standard pre-authentication: IEEE 802.11f/i/r

In IEEE 802.11f [17], an STA maintains association with a single AP and transfers security context information through the CAP to the TAP. This protocol is not directly applicable for inter-domain HOs and only covers intra-ESS HOs [18]. Moreover, IEEE 802.11f was not approved as a full-use standard protocol owing to its unsuitability. As alternative enhancements, IEEE 802.11i/r were ratified to support secure roaming to the TAP through pre-authentication with a key management mechanism [19,20]. The IEEE 802.11i standard has been included in the revised edition of the IEEE standard 802.11 since June, 2007 [21]. Pre-authentication of IEEE 802.11i/r enables an STA to establish a pairwise master key security association (PMKSA) with a new AP through the CAP. Once the STA successfully authenticates the new AP, the STA completes pre-authentication with a PMKSA between the STA and the TAP without performing a four-way handshake. When the STA actually roams to the coverage area of the TAP, it sends a re-association request message including the PMKSA name to the TAP. If the TAP successfully sends an association response message, the STA and the TAP directly perform a four-way handshake. In this manner, pre-authentication enables the establishment of PMKSA before an STA associates with a TAP (L2HO). At the same time, the STA can mitigate the delay due to pre-authentication with the TAP. Pre-authentication, however, has limitations, such as overloading on the centralized authentication server (AAA server) with an increase in the number of pre-authentication requests. Moreover, as pre-authentication is performed at the IEEE 802 layer (L2), it cannot be applied across IP subnets (L3) or different administrative domains.

These intra-ESS technologies have three problems when applied to current and future wireless networks. First, the existing protocols especially designed for the WLAN architecture are not applicable to inter-ESS and inter-domain authentication over a 3G-WLAN architecture. Mobile users have to perform HO to seamlessly continue services regardless of the ESS or domains in the context of the 3G-WLAN interworking architecture. However, 3GPP does not specify details on WLAN HH in 3G-WLAN interworking scenario. Thus, the EAP-AKA protocol is invoked whenever an HH occurs. EAP-AKA is an extensible authentication protocol (EAP) mechanism for authentication and session key distribution using Authentication and Key Agreement (AKA) mechanism. Second, for deployment, previous standard protocols need to be modified on the AP or AAA servers on the network side. This means that the currently installed equipments must be replaced, which is definitely cost ineffective for building commercial networks. Third, when the STA moves at a high speed out of the coverage area of the CAP, the transaction of pre-authentication cannot be completed owing to the fact that the STA loses connectivity with the APs. Hence, sufficient time should be allocated for pre-authentication so that the mobile STA can authenticate the APs.

2.2.2 IEEE 802.1X and EAP

IEEE 802.1X is a port-based network access control protocol that is used to establish mutual authentication and works as an efficient key exchange mechanism between STAs and authentication servers in wired and wireless LANs [22]. This protocol uses EAP messages to handle authentication requests and replies. EAP messages are extensible as they can be used for different authentication methods with IEEE 802.1X, such as login user names and passwords, smart cards, and digital certificates. The EAP procedure may include several round-trip message exchanges between the STAs and the AAA servers. Although the signaling overhead is determined by the network topology, in most cases, these signaling messages should be reached to the AAA server in the home domain before the STAs can access network services on a new network. Table 1 shows an experimental results that the association and authentication/authorization procedure in 3G-WLAN interworking scenario brings a huge amount of delay approximately in 4.3 s.

The parameters listed in the above table are defined as follows:

- α, β, and γ: the scope of authentication being performed in Figure 1 where denotes intra-ESS, intra-AAA, and inter AAA, respectively

Table 1 Comparison of the delay of security protocols (ms)

Scope	α	α	β	γ
Protocol	**WEP**	**WPA2-P**	**WPA2-E**	**3G-WLAN**
	-	**802.11i**	**EAP-GTK**	**EAP-AKA**
$T_{\text{open\_auth}}$	1.2	0.9	1.1	0.9
T_{asso}	2.1	1.2	3.8	2.3
T_{EAP}	-	-	732.8	4313.5
T_{4WHS}	-	27.6	21.9	71.1
$T_{\text{4WHS}} + T_{\text{asso}}$	-	28.8	25.7	73.4
T_{sum}	3.3	29.7	759.6	4387.8

- T_{open} auth: average time taken to authenticate using the open authentication method
- T_{asso}: average time taken to associate with the APs
- T_{EAP}: average time from EAPOL-start message to EAP-success
- T_{4WHS}: average time taken for a four-way handshake between the STA and the APs
- T_{sum}: summation of time at each phase

The average delays for protocols WEP, WPA2-Personal, and WAP2-Enterprise (EAP-GTK: generic token card) were measured at the Yonsei University and that for protocol EAP-AKA was measured at SK Telecommunications, South Korea. The average delay for each protocol was measured five times.

2.2.3 MPA: media independent pre-authentication

Dutta et al. [8] consider mobility management protocols as well as provide schemes for optimizing the inter-domain and inter-technology HO. MPA is a mobile-assisted and secure HO optimization scheme that can be applied to any link layer and is compatible with any mobility management protocol. In MPA, pre-authentication is assumed to be performed by the protocol for carrying authentication for network access (PANA) [23]. Two keys derived from the authentication agent and used to protect subsequent signaling messages are securely delivered to the configuration agent and the access router. Further, they assumed that the STA could find a target network through IEEE 802.21's media-independent information service. MPA is useful in view of the integration of L2 and L3 authentication. However, to apply this scheme to existing network architectures, i. e., the 3G-WLAN interworking architecture, it requires significant modifications of the infrastructure or hardware replacements which dramatically increase the cost inefficiency.

3 Proposed pre-authentication scheme

The proposed pre-authentication scheme enables the STA to authenticate a pre-determined AP once it has decided to roam. This scheme can minimize the overall HO time, thus effectively mitigates the service disruption of delay-sensitive applications.

3.1 Assumptions

First, we assumed certain conditions in the proposed pre-authentication scheme. Most of the assumptions are based on the interworking architecture shown in Figure 1.

i) An STA trusts the WLAN AAA (WAAA) and the Home AAA (HAAA) with which the STA is associated.
ii) Each WAAA must have a security association and roaming agreements with the HAAA in the 3G network.
iii) An STA can obtain information regarding the TAP, including its current status information such as a Beacon interval (BI), channel rate, and frequency through active and passive scanning schemes (e.g., proactive scanning [10], SyncScan [12]) or any other 3rd party entity provided by IEEE 802.21 standard [8].

3.2 Channel switching period (CSP)

We introduce a conceptual time slot, namely, the CSP, to allow an STA to interleave processes between data packet exchange with a CAP and pre-authentication with a TAP before triggering an HO. Specifically, the activated CSP is a processing period for the authentication tasks in a view of a TAP and also a buffering period for frames destined to the STA to the a view of a CAP in parallel. The CSP can be allocated with the STA, depending on the time required to complete the tasks. We also define the tasks between the STAs and the APs, such as association and authentication, as *transactions*. The CSP begins when channel switching occurs and ends when the STAs return their channel back to the original one. To support successive transactions, CSP operations, namely, channel switching and PSM operations are repeated. The overall CSP allocation flow is shown in Figure 3. Until the completion of the transactions, the additional CSPs will be allocated to the transactions in a loop. By checking the TIM field of the beacon frame at every LI, the STA can acquire its frames from the APs. When the STA receives the *Success* or *Fail* frame from TAP, the STA will exit the CSP loop. The LI informs the AP how often the STA wakes up from PSM to receive buffered frames from the AP, as well as allows the STAs to indicate how long the AP must retain the buffered frames. On other word, higher LI requires more AP memory size for per-STA frame buffering. We will discuss the trade off between the LI and AP's buffer memory size in Section 4.5.1. To describe the operation of the proposed scheme, first, two new operations are defined. Before describing the pre-authentication procedure in detail, we briefly introduce `CSP.begin` and `CSP.end` operations.

The `CSP.begin` operation consists of

i) sending of a PS-Poll frame to the CAP with PM = 1 (buffering data),
ii) switching of the channel to the TAP, and
iii) sending of a PS-Poll frame to the TAP with PM = 0.

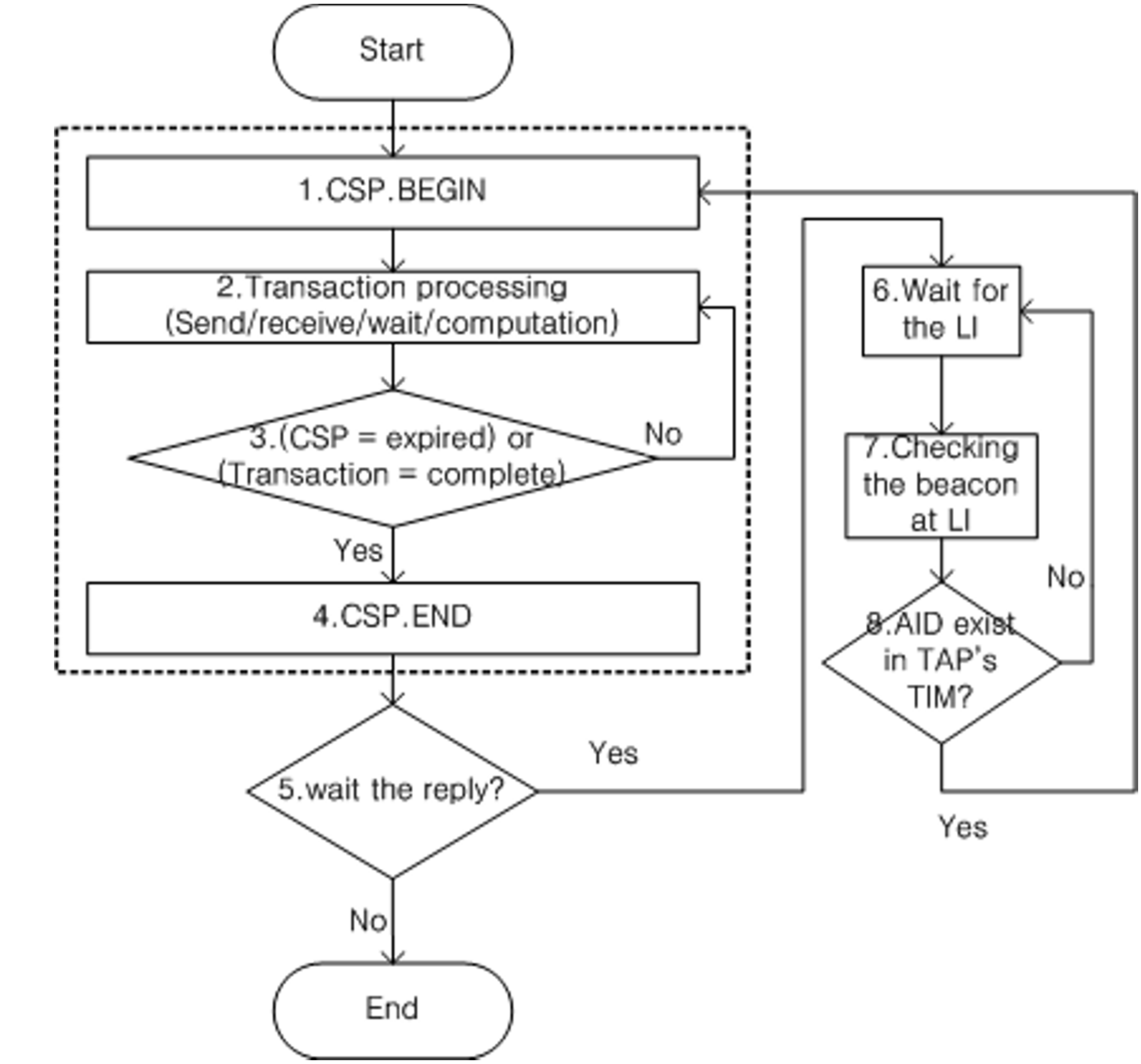

Figure 3 CSP allocation flow chart.

while the CSP.end operation consists of

i) sending of a PS-Poll frame to the TAP with PM = 1,
ii) switching of the channel back to the CAP, and
iii) sending of a PS-Poll frame to the CAP with PM = 0 (forwarding data).

3.3 Three phases of pre-authentication

We use the aforementioned CSP operations to reduce the authentication delay. That is to say, the proposed pre-authentication scheme allocates the CSPs using channel switching to exchange messages and uses the buffering function of the AP's PSM to prevent frame loss during pre-authentication. The basic pre-authentication procedures of the proposed scheme are depicted in Figure 4. The overall pre-authentication operation can be split into three distinct phases, namely *pre-authentication initiation*, *pre-authentication execution*, and *completion and L2 HO*.

3.3.1 Pre-authentication initiation phase

Initially, the STA communicates with the CAP on the basis of the assumptions presented in Section 3.1. When an STA enters an HO region, it ascertains its location and mobility rate required for pre-authentication (described in Section 4.3. When the STA decides to begin pre-authentication, it requests and receives information regarding the TAP (i.e., service set identifier (SSID)) via the information server such as IEEE 802.21.

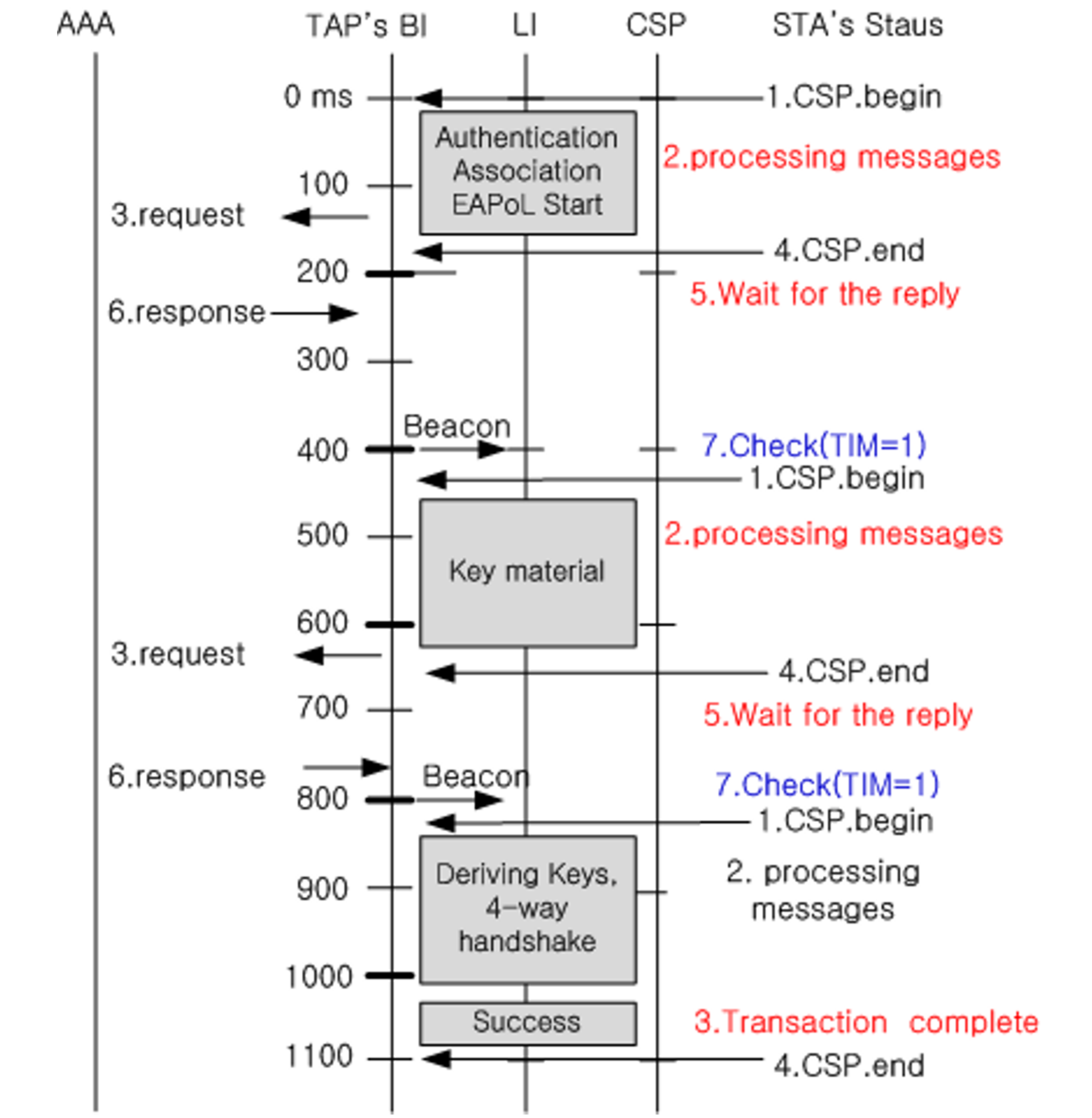

Figure 4 Basic operation concept.

3.3.2 Pre-authentication execution phase

After the pre-authentication initiation phase, the STA initiates the pre-authentication execution phase by performing the CSP.begin operation with the CAP and TAP (operation 1 shown in Figure 4). In this phase, the STA transmits pre-authentication request message (same as the normal EAP request message) to the TAP, and the TAP then relays this message to the AAA to request for 802.1X/EAP authentication (operation 5). This message contains the STA authentication information that is required for standard 802.1X/EAP authentication [24]. When the TAP receives an authentication request message from the STA, it begins EAP-AKA authentication on the basis of the messages received. Finally, the STA performs the CSP.end operation to switch back to the original channel and maintains the current session with the CAP. The average overall delay of the EAP-AKA authentication procedure was approximately 4.3 s in the 3G-WLAN downward HO (Table 1). Hence, until the authentication transactions are completed, the additional CSP manages the transactions, and subsequent messages are exchanged to complete the pre-authentication phase.

3.3.3 Completion and L2 HO phase

After the pre-authentication execution phase is successfully completed according to the standard authentication process, an EAP success message is transmitted to the AP along with authentication keying material such as pairwise master key (PMK). The AP buffers the received EAP success information so as to send it to the corresponding STA at the pre-defined LI during the next CSP. The STA periodically checks the TIM field for beacon frames coming from the TAP for receiving the result of authentication during each CSP (operation 7 in Figure 4). When the STA confirms that the TIM field in the beacon frame is set at a certain CSP, it immediately sends a PS-Poll frame to the TAP and receives all the frames it is expected to receive. Otherwise, the STA performs this operation (waiting and checking for beacon frame) periodically. After a specified number of iterations of the CSP, the STA can complete the transaction (operation 5). Thereafter, the STA detaches from the CAP while attaches to the TAP by using standard WLAN re-association procedures. That is, L2 HO is carried out from the CAP to the TAP. During this attachment process, the WLAN confirms that the STA is the pre-authenticated user from the previously received EAP success message. Therefore, the STA is able to communicate with the TAP via the WLAN Access Network (AN) immediately without any additional WLAN authentication process.

3.4 EAP-AKA example

Figure 5 shows an example of the EAP-AKA processing message flow in the proposed scheme when the CSP is 2 × *LI*, 200 ms. The EAP-AKA is the recommended standard protocol in the 3G-WLAN interworking architecture. In the first CSP, the STA requests authentication via the WAAA to the HAAA. The AAA server retrieves the STA's information from the HSS and sends the Authentication Vector (AV) to the TAP, including a random challenge (RAND), the authentication token (AUTN), the expected response (SRES), the encryption key (CK) and the integrity key (IK). At this point, the

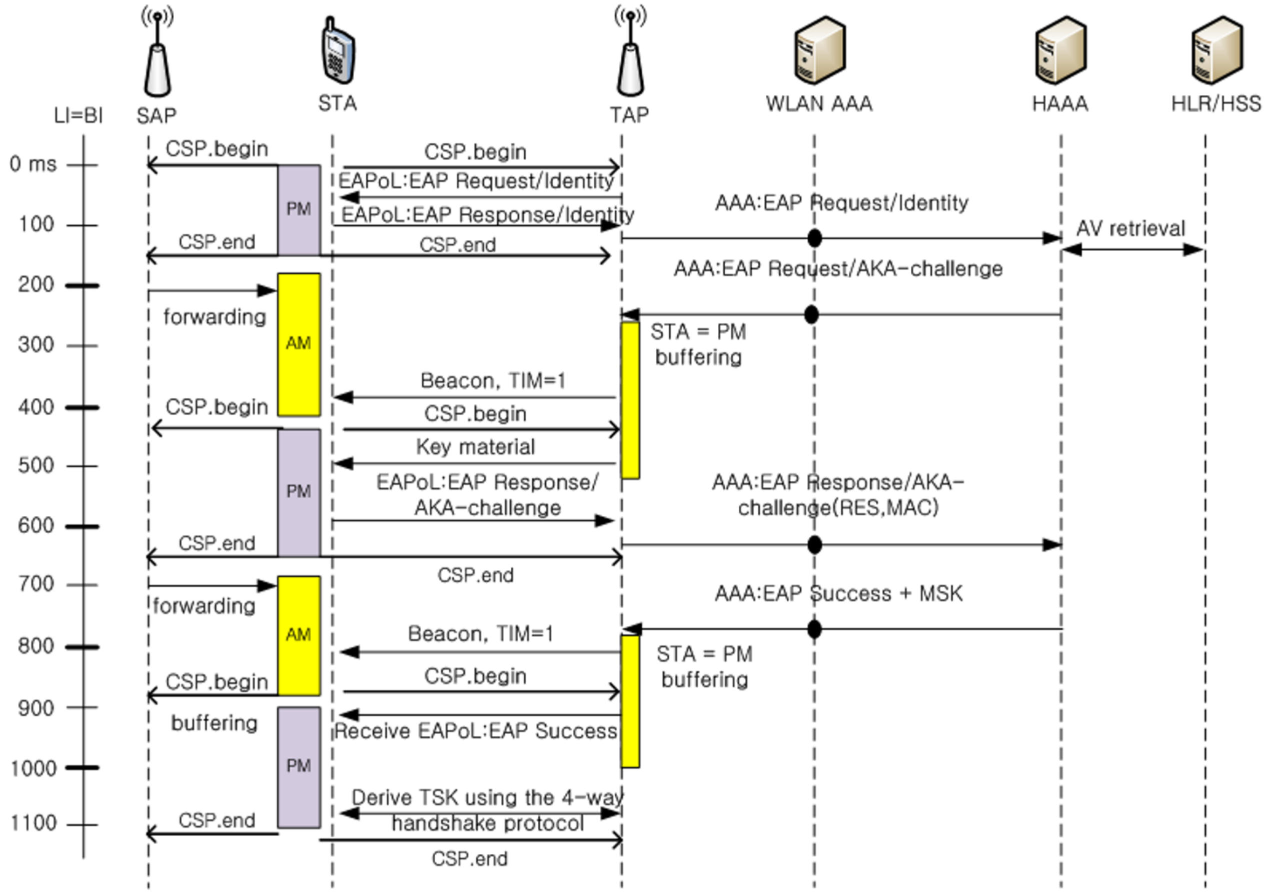

Figure 5 Proposed scheme procedure in EAP-AKA.

STA is in the PM; thus, the TAP has to buffer the data until the STA is in the AM. In the second CSP, the STA is in the AM with respect to the TAP; thus, the TAP now forwards the data.

4 Evaluation and analysis

This section evaluates the performance of the proposed pre-authentication scheme, which is based on fast channel switching in 3G-WLAN HH. We have analyze EAP-AKA in detail in terms of authentication delay, signaling cost, and mobility rate. Initially, the STA is connected to AP1 in domain A, as depicted in Figure 6. The STA then performs three intra-ESS HHs to APs 2, 3, and 4 in domain A. Then, it performs an inter-domain HH to AP5 in domain B, followed by two intra-ESS HHs to APs 6,7, and 8 in domain B. The performance of the proposed scheme is evaluated by comparing it with the performances of the three standard 802.11 roaming schemes [17,19,20]. It is difficult to accurately measure the performance of the proposed scheme with respect to HOs, because HO is affected by various factors such as dynamic network topology and node location changes. We thus present a numerical method to analyze the performance of the schemes in an accurate and reasonable manner within a realistic 3G-WLAN interworking architecture, as well as compare the proposed scheme with the conventional schemes. In addition to the assumptions made in Section 3.1, we make the following assumptions for evaluation purposes:

- The STA moves in a fixed path from domain A to domain B, as shown in Figure 6.
- The user of the STA uses a real-time broadcasting service from an Internet website, continuously.

When the APs are densely deployed, their network providers are usually different from each other. In other words, STAs are required to perform inter-ESS and inter-domain HOs. The analysis parameters are listed in Tables 2 and 3. Let $T_w(l, h_{x\text{-}y})$ denotes the transmission delay of a message with length l sent from x to y via wired links. $h_{x\text{-}y}$ is the number of hops separating x and y in the wired links. $T_w(l, h_{x\text{-}y})$ can be expressed as follows:

$$T_{\mathrm{w}}(l, h_{x-y}) = h_{x-y} \times \left(\frac{l}{B_{\mathrm{w1}}} + L_{\mathrm{w}}\right) + (h_{x-y} + 1) \times P_t \quad (1)$$

The transmission delay of a message with length l sent from an STA via a wireless link, $T_{\mathrm{wl}}(l)$, is given by

$$T_{\mathrm{w1}}(l) = \frac{l}{B_{\mathrm{w1}}} + L_{\mathrm{w1}} \quad (2)$$

The transmission delay of EAP messages via a wireless link and a wired link, T_{EAP}, is given by

$$T_{\mathrm{EAP}} = T_{\mathrm{w1}}(\mathrm{EAP}_{\mathrm{w1}}) + T_{\mathrm{w}}(\mathrm{EAP}_{\mathrm{w}}, d_{\mathrm{TAP\,-\,AAA}}) \quad (3)$$

4.1 Total authentication delay

Authentication delay plays an important role in the total HO delay. In this study, we assume that the AP scanning delay and the L3 delay have the same effect on all schemes. Authentication delay is calculated from the time the EAP Request/Identity message is sent to the time when a four-way handshake protocol is invoked, as shown in Figure 5. The total authentication delay is denoted by D. For an STA that performs HO, the total authentication delay for each scheme is given by the following equations:

$$D_b = 7 \cdot (T_{\mathrm{L2HO}} + T_{\mathrm{EAP}}) \times N_m \quad (4)$$

$$D_c = \frac{3}{7} \cdot P_b + 4 \cdot (T_{\mathrm{EAP}} + T_{\mathrm{w}}(\mathrm{sec\_cxt}, d_{\mathrm{CAP\,-\,TAP}}) + T_{\mathrm{L2HO}} + T_{\mathrm{4WHS}}) \times N_m \quad (5)$$

$$D_i = \frac{3}{7} \cdot P_b + 4 \cdot (T_{\mathrm{EAP}} + T_{\mathrm{L2HO}} + T_{\mathrm{4WHS}}) \times N_m \quad (6)$$

$$D_p = 7 \cdot (n \times T_{\mathrm{CSP}} + T_{\mathrm{w1}}(\mathrm{EAP}_{\mathrm{w1}}) + T_{\mathrm{L2HO}} + T_{\mathrm{4WHS}}) \times N_m \quad (7)$$

Equation (4) shows the basic 802.11 open system authentication (OSA) case without pre-authentication. The IEEE 802.11 takes a hard handoff *break-before-make* approach fundamentally, which means that an STA has to break its connection with its CAP before connecting to a TAP [25]. That is, the connection is disrupted during every HO. Thus, the total authentication delay in this case is the largest. Equation (5) shows the case of the context transfer scheme such as the trial standard IEEE 802.11f IAPP withdrawn on 2006. In this protocol, *break-before-make* movements occur three times in inter-ESS HOs, and *make-before-break* movements occur four times in inter-subnet HOs. An STA should transfer the security context to the TAP via the CAP, beforehand. Equation (6) shows the standard 802.11i intra-ESS pre-authentication case referred to as RSNA. In this case, *break-before-make* movements occur three times in inter-ESS HOs, and *make-before-break* movements that perform pre-authentication using PMKSA via the CAP indirectly occur four times in intra-ESS HOs. Equation (7) mathematically describes the case of the proposed scheme, which performs pre-authentication with the TAP directly beyond the border of the ESS. In this case, only the CSP operation time is needed, and not the EAP processing time.

The parameters used in this analysis are listed in Table 4. Some of the parameter values are taken from

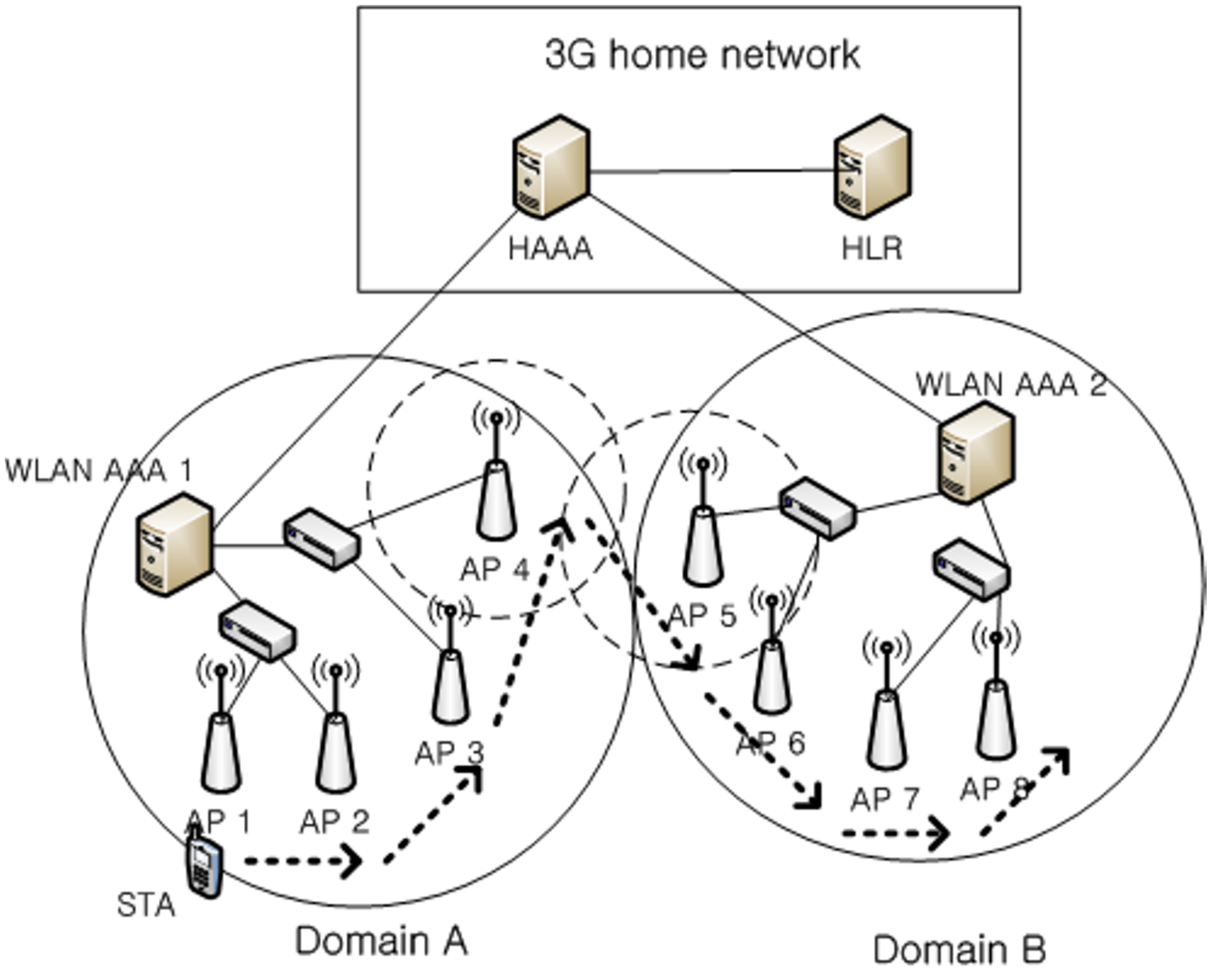

Figure 6 Evaluation network model and scenario.

articles [2,26]. In this study, however, we set the processing delay P_t to 400 ms because of the EAP-AKA processing of generating authentication vectors and keys in HSS and Universal Subscriber Identity Module (USIM). The values of $h_{x\text{-}y}$ are shown in Figure 6. Moreover, the total number of hops needed for EAP authentication and an L2 HO is assumed to be 3 and 1, respectively.

Figure 7 shows a plot of the total authentication delay against the STA resident time. As shown in this fugure, the total authentication delay decreases with an increase in the STA resident time. Further, authentication delay is greater in the basic 802.11 OSA than in the case of other pre-authentication schemes, because it has the longest duration of disruption during an HO. Context

Table 2 Parameters for Analysis 1

Parameter	Description
N_{STA_HAAA}	the number of EAP-AKA messages exchanged between an STA and HAAA
N_{STA_WAAA}	the number of EAP-AKA messages exchanged between an STA and WAAA
$N_{inter\text{-}ESS}$	the number of authentication messages exchanged for inter-ESS HO
$N_{intra\text{-}ESS}$	the number of authentication messages exchanged for intra-ESS HO
N_{csp}	the number of CSP messages exchanged for inter-ESS HO
S	the average authentication size

Table 3 Parameters for Analysis 2

Parameter	Description
l	Length of message
T_c	Average session connection time
T_r	Average WLAN cell resident time
N_m	Average number of movements in session, *i.e.*, $N_m = \lceil T_c/T_r \rceil - 1$
LI	LI
n	Total number of CSP during HOs, *i.e.*, $n = \lceil T_{EAP}/LI \rceil$
B_w	Bandwidth of wired link
B_{wl}	Bandwidth of wireless link
L_w	Latency of wired link (propagation delay and L2 delay)
L_{wl}	Latency of wireless link (propagation delay and L2 delay)
P_t	Routing table lookup and processing delay
EAP_w	The total length of EAP-AKA messages exchanged in wired link
EAP_{wl}	The total length of EAP-AKA messages exchanged in wireless link
T_{CSP}	Average time need for CSP operations
T_{L2HO}	Average time need for L2 HO
T_{4WHS}	Average time need for 4-way handshake
sec_cxt	Security context transferred from CAP to TAP

transfer schemes such as 802.11f show similar performances with 801.11 OSA because the transmission time of the security context is overloaded between two APs. The proposed scheme achieves the best performance because its duration of disruption is shorter than that of the other schemes. Therefore, the proposed scheme can ensure a low authentication delay, because its pre-authentication processes enable a fast HO.

4.2 Authentication signaling cost

The signaling cost introduced by an authentication process is an important metric for evaluating its performance. The authentication signaling cost is the accumulative traffic load introduced in the network by exchanging authentication signals during a communication session [2]. We compare our proposed scheme with conventional schemes. The authentication signaling cost associated with authentication during a session is denoted by *C*. On the basis of the movement scenario shown in Figure 6, *C* in the basic 802.11 OSA, 802.11f, 802.11i, and the proposed scheme can be calculated as follows:

$$C_b = (8 \cdot N_{\text{STA\_HAAA}}) \times S \times N_m \quad (8)$$

$$C_f = C_i = (2 \cdot N_{\text{STA\_HAAA}} + 4 \cdot N_{\text{intra - ESS}} + 2 \cdot N_{\text{inter - ESS}}) \times S \times N_m \quad (9)$$

$$C_p = (2 \cdot N_{\text{STA\_HAAA}} + 7 \cdot N_{\text{csp}} + 6 \cdot N_{\text{STA\_WAAA}}) \times S \times N_m \quad (10)$$

Table 4 Parameter setting

Parameter	Value	Parameter	Value
T_c	1,000 s	L_w	0.5 ms
T_r	2 ~ 40 s	L_{wl}	2 ms
T_{L2HO}	10 ms	EAP_w	150 bytes
T_{4HWS}	30 ms	EAP_{wl}	145 bytes
T_{CSP}	20 ms	Sec_ctx	114 bytes
P_t	400 ms	B_{wl}	11 Mbps

Equation (8) implies that the basic 802.11 OSA is used. The STA performs EAP-AKA authentication whenever it starts communicating with an AP, irrespective of whether an HH was performed or not. Equation (9) implies that 802.11f IAPP and 802.11i RSNA standard pre-authentication protocols are executed. These two standard schemes usually exchange the pre-authentication messages between the CAP and the TAP via the common Distribution System (DS) which connects APs in an ESS. Thus, we simply assume that the signaling cost of the two schemes is the same. These schemes perform full EAP-AKA authentication twice, context transfers (intra-ESS HH) four times, and inter-ESS HH in an intra-domain twice. Equation (10) refers to the case of our proposed scheme where pre-authentication based on fast channel switching occurs seven times with CSP operations. When the STA enters domains A and B, full EAP-AKA authentication must be performed twice for inter-domain HOs, and fast re-authentication must be performed six times for the other sections (pre-authentication within a domain without the need for contacting the 3G HAAA). The value of S is set to 100 bytes; T_r varies from 2 to 40 s. Figure 8 shows a plot of the authentication signaling cost against the STA resident time. It is generally observed that the longer the STA resident time, the lower is the number of generated authentication signals. Now, because our proposed scheme uses the CSP operation to directly pre-authenticate the TAP, the number of authentication signals generated by our proposed scheme is greater than that generated by conventional standard schemes. However, IEEE 802.11f

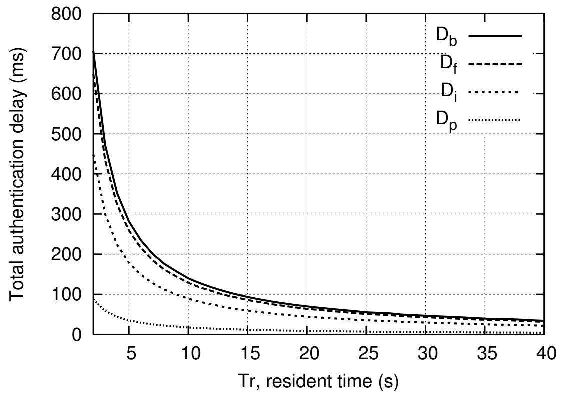

Figure 7 Total lost packet vs. STA resident time.

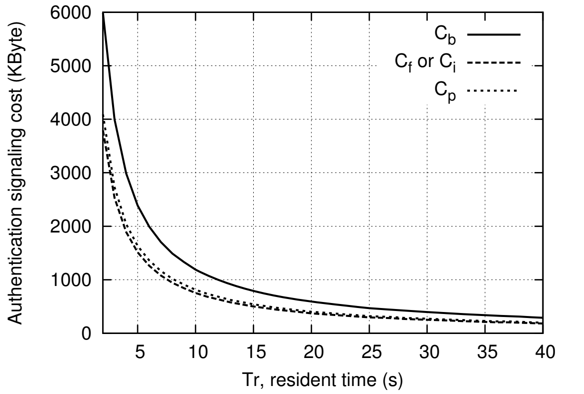

Figure 8 Authentication signaling cost vs. STA resident time.

and 802.11i need to transfer context information between APs. Moreover, as they cannot support inter-ESS and inter-domain HHs, they require a greater number of EAP-AKA authentication signals than our proposed scheme. Therefore, our proposed scheme reduces the signaling cost by an average of 32% of IEEE 802.11 OSA and increases the signaling cost by an average of 8% in comparison to the IEEE 802.11f and 802.11i.

4.3 Mobility rate

In this section, we analyze the difference between direct and indirect pre-authentication in terms of the mobility rate (velocity). In scenarios where the STA moves at high speeds, the STA performs HOs frequently; it should be noted that the time between two HOs must be sufficiently long to allow the completion of pre-authentication. The duration between two successive HOs/hl depends on the size of the wireless cell and the speed of the moving STA. In the case of indirect pre-authentication, the STA cannot go beyond the radio coverage of CAPs to pre-authenticate the TAP. Contrarily, in the case of direct pre-authentication, the STA can go beyond the coverage area of the CAPs to perform pre-authentication. Because the valid radio coverage for pre-authentication is extended to the coverage area of TAPs, the STA could speed up higher than the STA based on the indirect pre-authentication relatively. The amount of time available for pre-authentication depends on both the degree of overlap between the coverage areas and the velocity of the STA. Here, we will analyze the impact of the radio coverage, time for pre-authentication, and the velocity of STAs.

In the example shown in Figure 9, let us consider an STA moving with a velocity of v; this station transitions between AP 1 and AP 2. The coverage overlap between the two APs is assumed to be *c*, and the diameter of each coverage area of two APs is d. Given these parameters, the time allocated for pre-authentication, *T*, must be less than or equal to *c*/v if loss of connectivity is to be avoided. For example, if *c* is 50 m, the scanning

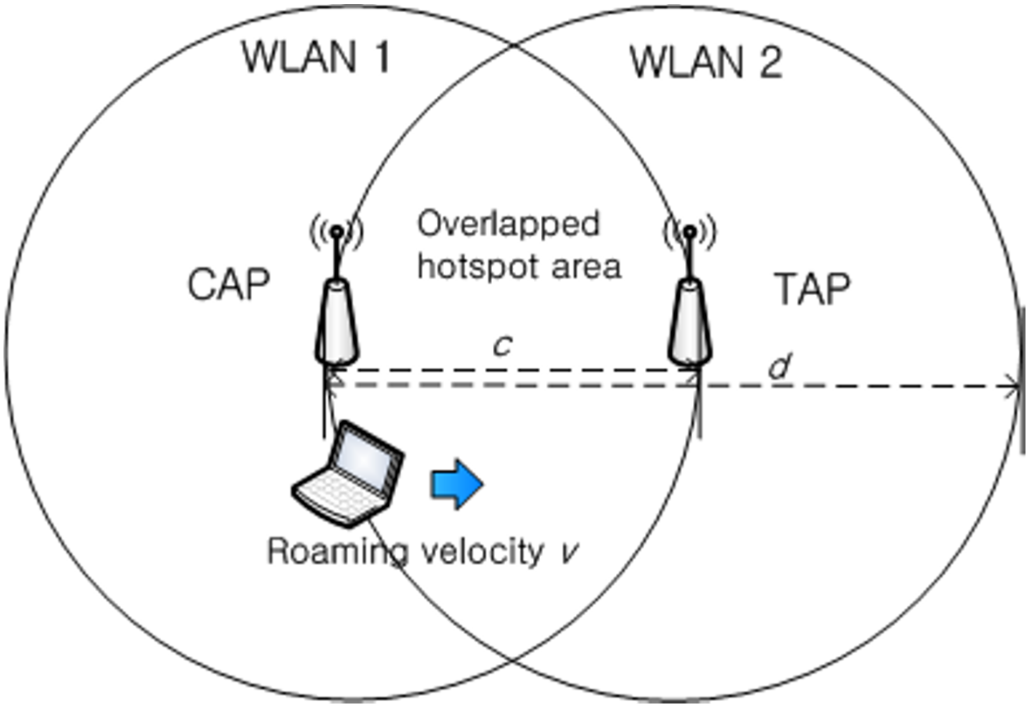

Figure 9 Mobility rate considerations in overlapped coverage.

delay time s is approximately 1000 ms and the pre-authentication delay time p is approximately 1000 ms. The maximum velocity supported by the access network is given by the following equation:

$$v_{\max} = \frac{c}{T} = \frac{(50/1000)\text{km}}{(2000/3600000)\text{h}} = 90\text{km/h} \tag{11}$$

where T is given by $s + p$ and is 2000 ms. Equation (11) shows that a mobile STA can perform indirect pre-authentication at a speed of up to 90 km/h. It is assumed that the STA initiates pre-authentication when it enters the coverage overlap area, where it detects the presence of AP 2.

$$v_{\max} = \frac{d}{T} = \frac{(150/1000)\text{km}}{(2000/3600000)\text{h}} = 270\text{km/h} \tag{12}$$

In contrast, as shown in Equation (12), the proposed direct pre-authentication scheme extends c to be equal to d of the coverage area of the TAP because of the fact that the STA performs direct authentication with TAP (usually, $c \leq d$). This means that the proposed scheme can support a mobility rate three times faster than supported by the direct conventional scheme. When the STA moves from one coverage area to another, in the case of the proposed scheme, the STA interacts directly with the TAP. As shown in Figure 10, when T = 2000 ms and c is roughly 50 m, the maximum velocity at which the STA can perform a successful HO is approximately 90 km/h, which is more than sufficient for daily operation. With an increase in the overlapping coverage area, i.e., with an increase in the number of TAPs, the maximum velocity of the STAs can be increased further. According to our experimental results, when T = 2000 ms and c = 90 m successful HOs can be made even at a $v_{\max}$ of 162 km/h. If we consider a densely deployed network topology, in which the AAA servers are very closely located and many network nodes belong to the same subnet, we can achieve HOs at very high STA velocities.

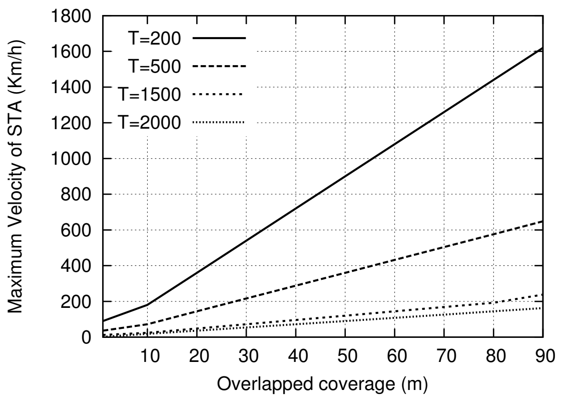

Figure 10 Mobility rate considerations in overlapped coverage.

4.4 Summary of performance analysis results

In this section, we summarize all the evaluation results based on the WLANs HH scenario shown in Figure 6 and provide a single metric to allow clear understanding of performance improvement.

As indicated in Table 5, the proposed CSP pre-authentication scheme is 5 to 7.8 times superior to the 802.11 OSA, 802.11f, and 802.11i standard protocols, respectively, when the mean delay time factor is considered. Additionally, the mean signaling cost of the proposed pre-authentication scheme is 32% less than that of 802.11 OSA and slightly more than that of the two standard protocols.

Therefore, the proposed pre-authentication scheme can minimize the authentication delay that occurs during intra-and inter-ESS HOs in 3G-WLAN interworking environments. It was also proved that the proposed pre-authentication scheme is more efficient than the existing authentication protocols in terms of the signaling cost.

4.5 Issues for consideration in the proposed pre-authentication scheme

4.5.1 Relationship between the QoS and the CSP duration

The CSP is composed of a number of LIs. At each LI, an STA has to wake up and check the beacon frame coming from the APs when operating in the PSM. However, the STA actually wakes up when it receives the CSP.begin message. This means that the CAPs have to buffer the data for the STA until the CSP.end message has been sent. CSPs have both the negative and the positive effects on the QoS. The short intervals of CSP consume much energy because of frequent channel switching, which causes a degradation in the QoS. On the other hand, the long interval of CSPs impose an additional overhead on the TAP, resulting in excessive buffering. However, it ensures that the response frames derived from the authentication procedures are successfully delivered to the CAP. The mobility of STAs can have a negative effect on the QoS, if they are not authenticated on time, owing to long CSP durations. If the STAs are not authenticated properly, the service could be disrupted, which could result in the degradation of the QoS. We define the relationship between the QoS and the CSP duration as follows:

Table 5 Summary of performance analysis results

Comparison parameters	802.11	802.11f	802.11i	Ours
Mean delay time (ms)	118	109	75	15
Mean signaling cost (Kbyte)	1001	634	634	684
Maximum speed of STA	-	-	*c/T*	*d/T*

$$\mathrm{BI} \leq \mathrm{STA}_{\mathrm{CSP}} \leq \frac{\mathrm{HO}_{\mathrm{distance}}}{\mathrm{STA}_{\mathrm{speed}}} \tag{13}$$

where $\mathrm{STA}_{\mathrm{CSP}}$ is the CSP of the STA, and $\mathrm{HO}_{\mathrm{distance}}$ is the distance from the current point to the maximum coverage point of the TAPs. The $\mathrm{STA}_{\mathrm{speed}}$ is the velocity of the STA. Equation (13) shows that $\mathrm{STA}_{\mathrm{CSP}}$ is inversely proportional to $\mathrm{STA}_{\mathrm{speed}}$ and directly proportional to $\mathrm{HO}_{\mathrm{distance}}$.

4.5.2 Security consideration

In this section, we cover specific threats introduced by the proposed pre-authentication scheme. Since our pre-authentication scheme involves the switching of channels between APs, we note the following security threats. First, a resource consumption denial-of-service attack is possible, where an attacker may send abnormal pre-authentication request messages to the candidate APs. As a result, the APs may spend computational and bandwidth resources on processing the pre-authentication messages sent by the attacker. To mitigate this attack, the candidate network or the authenticator (AP) may apply packet filtering so that only pre-authentication messages received from a specific set of serving networks or authenticators are processed.

Second, some consideration of the channel binding problem described in [27,28] is needed, as a lack of channel binding may enable an AP to impersonate another AP or communicate incorrect information via out-of-band mechanisms (such as via AAA or lower-layer protocols) [29]. Channel binding is a secure mechanism for ensuring that a subset of the parameters transmitted by the AP is agreed upon by the EAP peer and the server. It should be noted that it is easier to launch such an impersonation attack when using pre-authentication than when using normal authentication, as an attacker does not need to be on the same physical link as the legitimate peer to send a pre-authentication trigger to the peer. Meanwhile our proposed pre-authentication scheme does not provide any key management and context transfer schemes among an STA, APs, and AAA servers. The proposed scheme is carried out in the link layer of STAs. It means L2 security protocol such as 802.11i RSNA can protect the CSP messages which used in our scheme. Therefore our proposed scheme has an equivalent level of security to the security method used in EAP.

5 Conclusions

We proposed a novel pre-authentication scheme based on fast channel switching that performs direct pre-authentication with the next AP, in advance. This scheme minimized the authentication delay time during HOs, as was clearly shown in Section 4. Moreover, as shown in our evaluation and analysis, the signaling cost has been considerably reduced. In addition, the proposed scheme is efficient in inter-ESS and inter-domain HOs. Further, it can be easily implemented in WLANs by simply modifying the device driver of the STAs. In other words, if there is any change in the authentication and encryption methods, our pre-authentication scheme will still work correctly because it does not involve any modification and encryption methods. Finally, our scheme takes into account the effects caused by direct pre-authentication with TAP and can efficiently support high mobility, which is a property that has not been considered in existing standard protocols. Therefore, we can conclude that our proposed scheme is a novel pre-authentication scheme for IEEE 802.11 WLANs that support a 3G-WLAN interworking architecture.

Acknowledgements
This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2009-0076476).

Author details
[1]Department of Computer Science, Yonsei University, Shinchon, Seoul, South Korea [2]Network R&D Laboratory, KT Corp., South Korea

Competing interests
The authors declare that they have no competing interests.

Received: 27 June 2011 Accepted: 9 February 2012
Published: 9 February 2012

References

1. H Choi, O Song, D Cho, A seamless handoff scheme for UMTS-WLAN interworking, in *IEEE Globecom 2004*. **3**, 1559–1564 (2004)
2. H Choi, O Song, D Cho, Seamless handoff Scheme based on pre-registration and pre-authentication for UMTS-WLAN interworking. Wirel. Personal Commun. **41**(3), 345–364 (2007). doi:10.1007/s11277-006-9146-2
3. K Ahmavaara, H Haverinen, R Pichna, Interworking architecture between 3GPP and WLAN systems. IEEE Commun. Mag. **41**(11), 74–81 (2003). doi:10.1109/MCOM.2003.1244926
4. 3GPP, 3GPP TS 23.234 (v10.0.0), 3GPP system to wireless local area network (WLAN) interworking; system description 2011, V10.0.0.
5. AAl Shidhani, VCM Leung, Pre-authentication schemes for UMTS-WLAN interworking. EURASIP J. Wirel. Commun. Netw (2009). doi:10.1155/2009/806563
6. A Mishra, M Shin, W Arbaugh, An empirical analysis of the IEEE 802.11 MAC layer handoff process. ACM SIGCOMM Comput Commun Rev. **33**(2), 93–102 (2003). doi:10.1145/956981.956990
7. Y Ohba, Q Wu, G Zorn, Extensible authentication protocol (EAP) early authentication problem statement. *RFC 5836 (Informational)*. Internet Engineering Task Force (2010), http://www.ietf.org/rfc/rfc5836.txt
8. A Dutta, D Famolari, S Das, Y Ohba, V Fajardo, K Taniuchi, R Lopez, H Schulzrinne, Media-independent pre-authentication supporting secure interdomain handoff optimization. IEEE Wirel. Commun. **15**(2), 55–64 (2008)
9. H Kwon, K Cheon, K Roh, A Park, USIM based authentication test-bed for UMTS-WLAN handoff, in *Proceedings of IEEE Infocom*, Citeseer, Barcelona, Spain, (2006)
10. H Wu, K Tan, Y Zhang, Q Zhang, Proactive scan: Fast handoff with smart triggers for 802.11 wireless LAN, in *IEEE INFOCOM, IEEE Communications Society*, vol. 7. Anchorage, Alaska, 749–757 (2007)
11. D Murray, M Dixon, T Koziniec, Scanning delays in 802.11 networks, in *Proceedings of The 2007 International Conference on Next Generation Mobile Applications, Services and Technologies*, IEEE Computer Society, Wales, UK, 255–260 (2007)

12. I Ramani, S Savage, SyncScan: practical fast handoff for 802.11 infrastructure networks, in *IEEE INFOCOM, Citeseer*. **1**, 675 (2005)
13. S Park, H Kim, C Park, J Kim, S Ko, Selective channel scanning for fast handoff in wireless LAN using neighbor graph. in *Personal Wireless Communications*, Springer, 629–629 (2004)
14. S Seo, J Song, H Wu, Y Zhang, Throughput-based MAC layer handoff in WLAN, in *Proceedings of the 28th IEEE international conference on Computer Communications Workshops*, IEEE Press, 409–410 (2009)
15. J Baek, S Seo, J Song, Multiple preauthentication schemes based on fast channel switching in public wireless LANs, in *International Conference on Innovations in Information Technology*, Al Ain, UAE, 16–20 (2009)
16. H Kim, D Cho, An Efficient power-saving protocol for internet traffic in wireless LANs, in *IEEE VTS Vehicular Technology Conference, IEEE Vehicular Technology Society*, vol. 62. Dallas, Texas, USA, 784–788 (2005)
17. IEEE trial-use recommended practice for multi-vendor access point interoperability via an inter-access point protocol across distribution systems supporting IEEE 802.11 operation. in *IEEE Standard for local and metropolitan area networks* (2003)
18. M Bargh, R Hulsebosch, E Eertink, A Prasad, H Wang, P Schoo, Fast authentication methods for handovers between IEEE 802.11 wireless LANs. in *Proceedings of the 2nd ACM international workshop on Wireless mobile applications and services on WLAN hotspots,* ACM 51–60 (2004)
19. 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. in *IEEE Std 802.11-2007 Revision of IEEE Std 802.11-1999*, 192–249 (2007)
20. IEEE Std 802.11r-2008 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008), 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 2: Fast Basic Service Set (BSS) c1–108 (2008)
21. Medium access control (MAC) and physical layer (PHY) specifications, IEEE standard 802.11-2007. in *IEEE Computer Society LAN MAN Standards Committee, Ed* (2007)
22. AAl Naamany, AAl Shidhani, H Bourdoucen, IEEE 802.11 wireless LAN security overview. IJCSNS6(5B) 138 (2006)
23. D Forsberg, Y Ohba, B Patil, H Tschofenig, A Yegin, RFC 5191 protocol for carrying authentication for network access (PANA). *Network Working Group* (2008)
24. 3GPP: 3GPP TS 33.234 (v11.0.0), 3G security; WLAN interworking security, System description. (2011) V11.0.0
25. J Chen, Y Tseng, H Lee, A seamless handoff mechanism for IEEE 802.11 WLANs supporting IEEE 802.11 i security enhancements. in *IEEE Asia-Pacific Wireless Communications Symposium* (2006)
26. S Lo, G Lee, W Chen, J Liu, Architecture for mobility and QoS support in all-IP wireless networks. IEEE J. Sel. Areas Commun. **22**(4), 691–705 (2004). doi:10.1109/JSAC.2004.825964
27. B Aboba, D Simon, P Eronen, RFC 5247-Extensible authentication protocol (EAP) key management framework, in *Network Working Group* (2008)
28. N Williams, RFC 5056-On the use of channel bindings to secure channels, in *Network Working Group* (2007)
29. B Aboba, L Blunk, J Vollbrecht, J Carlson, H Levkowetz, RFC 3748-Extensible authentication protocol (EAP), in *Network Working Group* (2004)

doi:10.1186/1687-1499-2012-39
Cite this article as: Baek *et al.*: A novel pre-authentication scheme based on fast channel switching in IEEE 802.11 WLANs. *EURASIP Journal on Wireless Communications and Networking* 2012 **2012**:39.