JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 26, 1345-1362 (2010)

Fast Handoff among IEEE 802.11r Mobility Domains*

KUANG-HUI CHI, CHIEN-CHAO TSENG+ AND YA-HSUAN TSAI+
Department of Electrical Engineering
National Yunlin University of Science and Technology
Touliu, 640 Taiwan
E-mail: chikh@yuntech.edu.tw
+*Institute of Computer Science and Engineering*
National Chiao Tung University
Hsinchu, 300 Taiwan
E-mail: {cctseng; yhtsai}@csie.nctu.edu.tw

This paper deals with secure fast handoff among access points (APs) of different IEEE 802.11r mobility domains. We leverage standard IEEE 802.11i mechanisms to let a station preauthenticate and establish a pairwise transient key with some target AP beforehand. Upon reassociation, the new AP aware of the preauthenticated station can thus complete handoff sooner than would otherwise be required. In order to resolve target APs timely, we introduce a location server that maintains network topology of an autonomous system covering multiple mobility domains. The location server assesses with which AP(s) the mobile station may reassociate next using its migration tendency. Accordingly the station is instructed to preauthenticate with fewer potential next APs than unnecessary. Performance discussions indicate that our proposal is effective in practice. Our approach is not only complementary to emerging IEEE 802.11r-based techniques but also useful to any network-layer fast handoff schemes for streamlined communication.

Keywords: wireless local area network, fast handoff, preauthentication, IEEE 802.11r, IEEE 802.11i

1. INTRODUCTION

This paper proposes an approach to speeding transitions of a station across different domains in IEEE 802.11 wireless networks. While a station wishes to retain access to Internet services over wireless media in course of movements, the small coverage of access points (APs) may lead the mobile station (MS) to suffer repeated traffic disruptions out of frequent handoffs. The handoff process occurs when a station migrates from one AP to another, involving AP discovery, authentication, reassociation, inter-AP context transfer for the mobile station, and a 4-Way Handshake whereby the MS and its new AP derive a shared cryptographic key for data delivery over the wireless medium. Among others, the authentication procedure refers to legacy open-system [1] and IEEE 802.1X authentications [12] that account for potentially prohibitive delay due to transactions at a remote site.

In order to bypass IEEE 802.1X authentications during handoff, several schemes were proposed, *e.g.*, [10, 11, 16] to name a few. State-of-the-art schemes are discussed in [8, 13]. As a most recent trend, IEEE 802.11r takes another avenue to achieve fast transi-

Received May 27, 2008; revised June 1, 2009; accepted October 22, 2009.
Communicated by Tei-Wei Kuo.
* This work has been supported by the National Science Council of Taiwan, R.O.C., under Grants No. NSC 98-2220-E-009-047 and NSC 97-2221-E-009-051-MY3.

tions of an MS among APs within a *mobility domain* – a managed set of APs sharing security associations [4]. When an MS first (re)associates in a mobility domain, IEEE 802.1X authentication remains required to establish the security context at the MS and its local AP. As exemplified in Fig. 1, after a mobile station authenticates via access point AP_I to its Authentication Server, the MS's security context is sent to and kept in AP_I. Such a context resulting from IEEE 802.1X authentication contains the Pairwise Master Key R0 (PMK-R0). PMK-R0 is then used to derive a second-level key, namely PMK-R1 key, whereupon the MS and its local AP compute a pairwise transient key for data encryption. (IEEE 802.11r defines a three-tier key hierarchy.) Later when roaming is expected to occur, a prospective AP acquires the MS's PMK-R1 key, if absent, from AP_I and caches the acquired key accordingly. Since PMK-R1 key acquisition and encryption key derivations are completed a priori, the MS can establish security association and reserve resources at its new AP ahead, minimizing connectivity loss due to handoff.

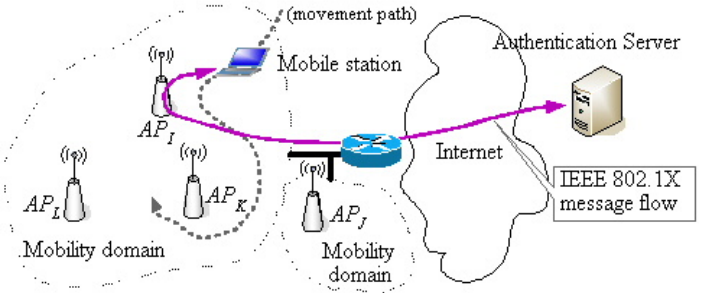


Fig. 1. Under IEEE 802.11r the first (re)association in a mobility domain requires IEEE 802.1X authentication. The established security context will be distributed from the first reassociated AP to other APs along with the MS's movement in the same domain whenever necessary.

Note that currently the IEEE 802.11r does not allow for movement among different mobility domains, *e.g.*, moving back and forth near the border between two domains. As a remedy, we contend with such mobility scenarios using standard IEEE 802.11i mechanisms to realize a new handshake procedure by preauthentication. Our approach keeps pre-established keying material for quick matching in some AP(s) of a new domain toward which an MS moves. The matched keying material is then used for data protection after handoff. Further, in order to resolve target APs, we introduce a location server that maintains network topology of an autonomous system. The location server assesses to which AP(s) an MS may reassociate more likely using the MS's migration tendency. This facilitates the MS to preauthenticate with fewer potential next APs than unnecessary. Overall, our approach provides an effective means, besides complement to IEEE 802.11r, underlying any network-layer fast handoff schemes as well.

We place emphasis on secure fast handoff that meets Robust Security Network requirements [3]. Unlike schemes relying on inter-AP security context transfers across mobility domains, our approach never divulges security-sensitive information to another party, nor over the network. Our objective is to prevent from trading performance for security and robustness to the extent that security requirements are unduly weakened. The remainder of this paper is organized as follows. The next section describes techniques to

be used in this study. Our approach is detailed in section 3. Section 4 discusses implementation considerations and performance results. Lastly section 5 concludes this paper.

2. BACKGROUND

IEEE 802.11r stipulates that each AP generate Beacon or Probe Response frames containing a Mobility Domain Identifier (MDID). APs of a same mobility domain share a unique MDID, which characterizes a region where an MS may roam among different APs providing IEEE 802.11r fast transition support. We consider henceforth that an MS is likely to reassociate with an AP belonging to another mobility domain, advertising a different MDID from that in current use by the MS. Under discussion is the provision of secure fast handoff for an MS performing inter-domain mobility.

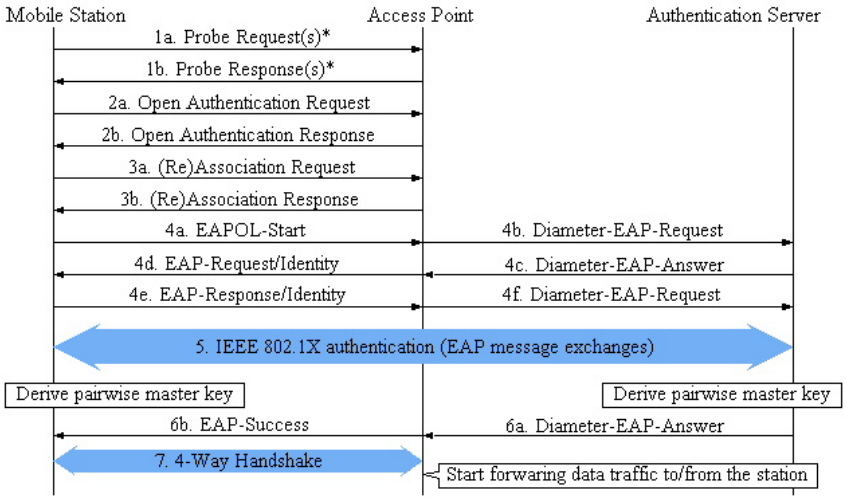


Fig. 2. Message flow for an MS handed off to an AP in standard IEEE 802.11i settings. Message marked with '*' may be not present.

Our development is based on IEEE 802.11i that defines standard mechanisms redressing security flaws of IEEE 802.11. As part of handoff to a new AP in IEEE 802.11i settings, an infrastructured network requires open-system and IEEE 802.1X authentications for access control (Fig. 2). In particular, IEEE 802.1X defines a framework allowing of various authentication methods over the Extensible Authentication Protocol (EAP) [7]. EAP messages carrying upper-layer authentication information are encapsulated in EAP over LAN (EAPOL) frames for wireless transport and in the Diameter protocol on the wired side, respectively. Here the AP bridging wireless and wired media acts as a transit entity to relay such authentication messages. A counterpart to Diameter is the RADIUS protocol (Remote Authentication Dial In User Service) [18].

IEEE 802.1X authentication is initiated with an EAPOL session start-up (step 4a of Fig. 2, followed by challenge-response interactions between a concerned MS and some backend Authentication Server (step 5). Interactions terminate successfully when these

two parties share a 256-bit pairwise master key. Then the Authentication Server sends the station's local AP a Diameter-EAP-Answer message with a result code and a payload containing the pairwise master key (step 6a). The receiving AP sends an EAP-Success message (step 6b) and proceeds to a 4-Way Handshake procedure. The handshake (step 7) involving four EAPOL frame exchanges between the AP and the MS confirms the possession of the pairwise master key whereby a pairwise transient key (PTK) is derived accordingly. PTK is used by IEEE 802.11i encryption protocols for protecting traffic over the wireless medium.

IEEE 802.11i allows preauthentication by letting an MS send via its current AP to some target AP an EAP-Start message as a conventional data frame, with the *EtherType* field set to 0x88C7. The target AP hence executes steps 4b to 6b of Fig. 2, except that interactions with the MS progress indirectly through its current AP. Successful preauthentication will lead the MS and target AP to cache the newly-generated pairwise master key in a data structure, namely pairwise master key security association. When reassociation occurs, the target AP can respond to the reassociating MS with an immediate EAP-Success message. Then a 4-Way Handshake can commence straightaway. It is noted that preauthentication involves the exchange of EAPOL-Start and EAP-Packet messages only.

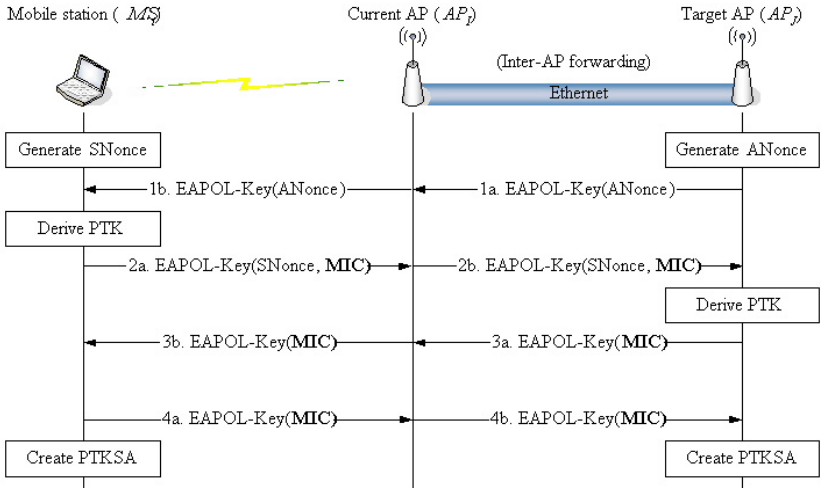
3. THE PROPOSED APPROACH

A handoff process involves three procedures: AP discovery, IEEE 802.1X authentication, and 4-Way Handshake. Toward fast handoff across APs of different mobility domains, we propose a pre-4-way handshake (or pre-handshake for short) procedure and the use of a location server, as shall be described next.

3.1 Pre-Handshake

In order to save PTK derivation during a handoff process, we carry out the 4-Way Handshake ahead of handoff. Our pre-handshake procedure is activated after the concerned MS has completed preauthentication with its target AP. The procedure operates essentially as the standard 4-Way Handshake yet with following distinctions.

- Because the MS has not yet reassociated with its target AP, pre-handshake messages are forwarded by its current AP. The pre-handshake is initiated by the target AP.
- EAPOL-Key frames for inter-AP forwarding are used in our architecture. We set the *EtherType* field of such frames to 0x88C7, different from the original 0x888E for IEEE 802.1X. Although our pre-handshake frames share the same Ethernet Type with those for preauthentication, frames remain distinguishable by their packet type in use. The packet type to our purpose is EAPOL-Key as opposed to EAP-Packet for preauthentication.
- Upon the completion of the pre-handshake, both the MS and target AP record the newly derived PTK in a data structure named PTKSA (PTK security association) [3]. In addition to PTK, PTKSA stores an identity for the security association, a pairwise cipher suite selector and machine addresses of these two parties. PTKSA is predefined in IEEE 802.11i.



(a) Pre-handshake message flow.

Message	Source address	Transmitter/ Receiver address	Destination address	Media	MIC protected
1a	AP_J	–	MS_i	wired	no
1b	AP_J	AP_I	MS_i	wireless	no
2a	MS_i	AP_I	AP_J	wireless	yes
2b	MS_i	–	AP_J	wired	yes
3a	AP_J	–	MS_i	wired	yes
3b	AP_J	AP_I	MS_i	wireless	yes
4a	MS_i	AP_I	AP_J	wireless	yes
4b	MS_i	–	AP_J	wired	yes

(b) Address fields of pre-handshake messages.

Fig. 3. Pre-handshake messages.

For convenience of exposition, let us consider a case where a local station MS_i of AP_I is conducting a pre-handshake with its target AP, say AP_J, belonging to another mobility domain. Fig. 3 (a) illustrates the handshake procedure as follows.

1. Thanks to preauthentication, both MS_i and AP_J share the same pairwise master key. We let AP_J generate and include ANonce, a random number, in a message addressed to MS_i via AP_I (message 1a). The message is forwarded later as message 1b to the destination.
2. Upon receipt of message 1b, MS_i generates SNonce, another random number, and uses the received ANonce to derive a PTK using some hash function as per IEEE 802.11i. Subsequently MS_i sends AP_J a message carrying message integrity code MIC (message 2a). MIC is used to protect the EAPOL-Key frame from undetectable alteration.
3. After message 2b arrives, AP_J derives a PTK using also the received SNonce and its own ANonce. With the PTK in place, the received message is checked whether to have a valid MIC. If so, AP_J sends a message to MS_i (message 3a). Otherwise, the handshake is terminated immediately.
4. On receiving message 3b, MS_i checks whether the carried MIC is correct. If yes, MS_i sends the fourth message back to AP_J (message 4a) signifying the handshake to be

completed at the MS side. When receiving message 4b, AP_J performs a MIC check. The handshake is completed at the AP side if the MIC is found correct.

Each prescribed message requires a replay check at the destination site as per IEEE 802.11i before any subsequent processing. A successful pre-handshake concludes with the creation of PTKSA on both sides. The standard data structure, PTKSA, of IEEE 802.11i is of avail to us for storing the result from a pre-handshake.

Fig. 3 (b) summarizes address fields of pre-handshake messages over which transmission medium. Note that inter-AP messages (over the wired medium) contain two address fields, so values of the corresponding Transmitter/Receiver Address column are absent. By comparison, messages for wireless transfer contain three address fields. For EAPOL-Key delivery across different media, frame conversion is required. Such conversion can be realized using encapsulation and decapsulation at AP_J and AP_I, respectively, in this scenario. To deliver an EAPOL-Key message to MS_i, AP_J encapsulates the message in a normal Ethernet frame; an outer IEEE 802.3 header is inserted in front of the original EAPOL-Key message. The outer header's Source Address and Destination Address specify AP_J's and AP_I's machine addresses, respectively, taken from indicated address fields of the EAPOL-Key message. Thus encapsulated frames will be received by AP_I via the IEEE 802.11 distribution system. On reception, AP_I examines whether the frame is intended for pre-handshake purpose, *i.e.*, whether *EtherType* carries 0x88C7 with packet type being EAPOL-Key. If so, the outer header is removed and the inner part (data payload) is further processed. Further processing refers to deciding for which station the EAPOL-Key message is destined, and then delivering the message to the intended station, MS_i.

On the contrary, AP_I can encapsulate an EAPOL-Key message for AP_J that performs decapsulation. This scenario corresponds to delivering messages 2b and 4b in Fig. 3. In practice, as AP_I receives an EAPOL-Key message from MS_i to AP_J, AP_I conveys the message in the payload part of an Ethernet frame. The frame header indicates AP_I and AP_J as sending and receiving machines, respectively. When the frame is received via the distribution system, AP_J examines whether the frame contains an EAPOL-Key message. If so, the message is extracted for pre-handshake processing. Essentially we augment the distribution system to support EAPOL-Key message delivery across APs.

3.2 Location Management

For timely preauthentication and pre-handshake, an MS can be made knowledgeable about its potential next APs. To this end, we introduce a location server similar to that in [19], yet with following functionality:

- The server is capable of collecting location information from MSs situated within its administrative domain.
- The server will resolve potential next APs for an MS on demand, based on network topology, MS's moving tendency, and/or policies of network providers.
- The server maintains AP-network topology that indicates not only *handoff-to* relationship among APs (provided by *neighbor graphs*[1]) but also channels in use by which APs.

[1] A neighbor graph is a data structure representing (re)association patterns of mobile stations among APs, which is useful to capture the traits or locality of mobility [10].

The provision of indicated channels enables an MS to shorten AP discovery delays. The administrative area of a location server generally comprise more than one mobility domain. We propose to co-situate the server at the local Authentication Server.

An MS is capable of learning of its current position and movement direction via any indoor-location techniques [17]. For pragmatic considerations, however, we let an MS measure received signal strengths (RSSs) from APs in radio range. These measures are reported collectively to the location server. With these signal reports, the location server can resolve potential next APs upon request by the MS whenever necessary. One way of resolving such APs is exemplified in Fig. 4. For each AP, consider two consecutive measures of RSSs sequentially. We mark a change of RSSs as '+' if a latter RSS is larger than or equal to its immediately preceding measure, or as '–' otherwise. In Fig. 4, for instance, we have changes of RSSs as a sequence "– + + – +" (3 +'s, 2 –'s) with respect to AP_J, while "– + + – +" (2 +'s, 3 –'s) with respect to AP_K. There are more +'s than –'s in the sequence concerning AP_J, so we expect the MS to have a higher likelihood of moving closer to AP_J, thereby reassociating with AP_J in the near future. Similar assessments lead us to infer that the MS is less likely to roam to AP_K next (because of +'s being fewer than –'s). Provided that the MS is currently local to AP_I, the location server can select AP_J but not AP_K as one of the potential next APs for the MS if (AP_I, AP_J) is an edge of the neighbor graph. As a refinement, we let the MS issue the request for prospective AP resolution when its received signal strength from the current AP has fallen below some threshold RSS_t.

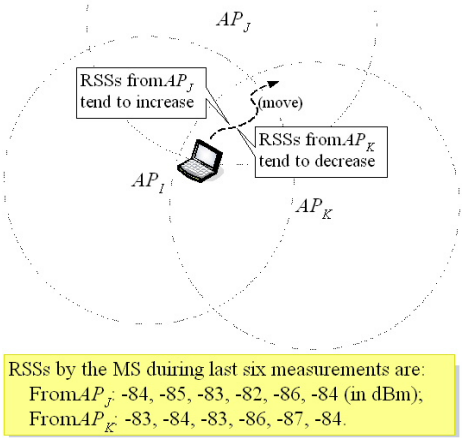


Fig. 4. Changes of RSSs by an MS with respective APs suggest to which APs the MS tends to reassociate next.

To allow for varying radio channel conditions and mobile direction uncertainty, the location server selects for a concerned MS n ($n \geq 1$) out of neighbor APs as next targets with most '+'s. Observe that a larger number n of target APs favor the MS doing fast handoff with a higher likelihood due to fewer mispredictions, yet at the expense of involving the MS and more APs in preauthentication and pre-handshake processes. A few selected APs, say $n = 2$, may cater for cost-effectiveness considerations.

It is stressed that RSS information is not the sole determinant of resolving potential next APs. Target AP resolution is also made with reference to the neighbor graph maintained by the location server itself. The neighbor graph indicates handoff-to relationship, a profile of each managed MS actually reassociating with which APs in the past. Besides, note that MS movement tends to exhibit some locality, implying that an MS may typically roam back and forth among certain APs. (For example, a user in daytime migrates mostly among certain offices on a regular basis.) Since such reassociation patterns are becoming stable over time, our resolution based on the resulting handoff-to relationship can thus gain better accuracy, with reduced mispredictions in the long run.

3.3 Reassociation Procedure

As mentioned, successful preauthentication and pre-handshake lead an MS and its target AP to share a pairwise master key and PTKSA, respectively. The former is indexed by the identity PMKID, whereas the latter by PTKID. Upon switch over to such an AP, the MS issues a Reassociation Request frame containing PTKID. The AP then uses the received PTKID to check whether the indicated PTKSA exists. If so, the PTK is retrieved for installation on the AP's wireless network interface. Subsequently the AP responds to the MS indicating a successful reassociation, which instructs the MS side to install the PTK as well.

However, if PTKSA does not exist, two possible cases follow. First, in case that the AP retains the pairwise master key, the AP still acknowledges the MS a Reassociation Response frame indicative of successful reassociation. In particular, the response frame contains a Status Code, say 2, dictating a 4-Way Handshake. Accordingly the MS performs the handshake to complete its handoff.

In the second case, the AP does not hold the pairwise master key. Then the Reassociation Response frame contains a Status Code indicating authentication failure. In that event, the MS must perform IEEE 802.1X authentication and a 4-Way Handshake as requested. Fig. 5 illustrates our fast handoff scheme as a whole.

3.4 Remarks

We observe that the notion of introducing a location server accords with a current trend of developing media-independent handover techniques (IEEE 802.21 [5]). A feasible implementation is to co-situate our location server at an IEEE 802.21 information server that provides information about networks in its administered area. The use of such a server enables MSs to learn necessary information like neighbor maps, link-layer parameters, and available services of APs prior to handoff. While an information server is generally maintained for an autonomous system, say a campus network, covering multiple mobility domains, the server accommodates MSs therein with information access. In view of the emerging standard IEEE 802.21 paradigm, any means to reduce implementation complexity and maintenance cost of an IEEE 802.21 information server applies well to our architecture.

Taking a campus network as an example autonomous system, a mobility domain may correspond to a department (sub)network of APs. A campus-wide location server can be set up for MSs performing fast handoff. Access to the server is made mainly when handoff becomes imminent, accounting for infrequent, small amount of traffic as compared

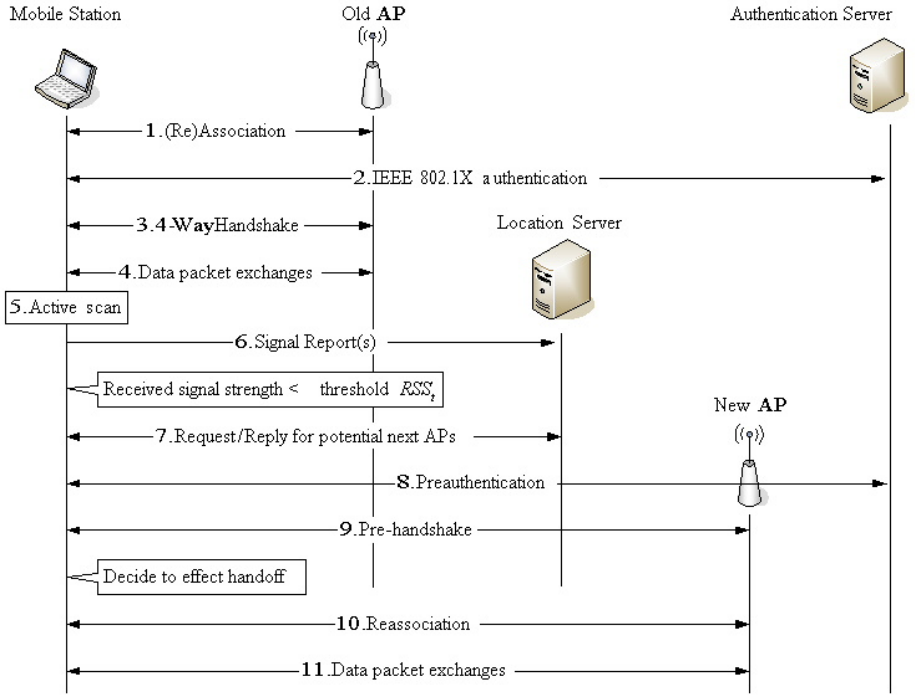
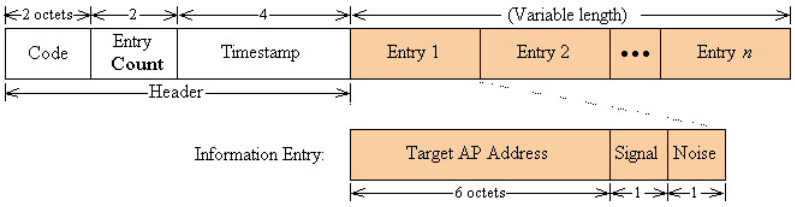


Fig. 5. Overall message flow of our proposed handoff process.

with normal data traffic. Therefore concurrent accesses by limited quantities of MSs doing handoff could hardly overwhelm the server. We believe that the location server appears neither much different from commonly used campus-wide servers such as RADIUS server in terms of operational principles, nor a costly add-on if co-located with an IEEE 802.1X Authentication Server. As our development is in line with IEEE 802.21 for the wireless Internet, the use of a location server is arguably practical to a certain extent.

In our architecture the location server for an autonomous system operates with foreknowledge of APs belonging to which mobility domains in its managed area. However, detailed topology of mobility domains is not required. Such information can be either pre-configured in or learned reactively by the location server when APs register with the regional Authentication Sever. In the latter, similar to IEEE 802.11F protocol initiation, registration takes place when an AP is powered on to perform certain message exchanges with the Authentication Server (*i.e.*, the region-governing RADIUS server) for establishing a secure communication channel in between. A registration message carries the address/identity and mobility domain identifier (predefined as per IEEE 802.11r) of the sending AP, whereby the Authentication Server learns the mapping between the AP and its affiliated mobility domain. Now that the location server has been co-situated with the Authentication Server (see section 3.3), the learned affiliation relationship of APs is readily accessible to the location server. Thus, when the location server resolves for an MS a prospective AP belonging to a different mobility domain from the current one the MS is visiting, an inter-mobility domain handoff will probably occur. Otherwise, an intra- mobility domain handoff procedure suffices, as per IEEE 802.11r.



(a) Generic message format for location information exchanges.

0x00	2	Timestamp	
00:05:4E:46:D1:E9		-68 dBm	-96 dBm
00:03:34:9A:05:A0		-66 dBm	-99 dBm

(b) Signal report.

0x01	0	Timestamp

(c) Request for prospective AP resolution.

0x02	3	Timestamp	
00:05:4E:46:D1:E9		0	0
00:03:34:9A:05:A0		0	0
00:01:B3:FF:00:11		0	0

(d) Reply of potential next APs.

Fig. 6. Message format and examples for location information exchanges.

4. DISCUSSION

In what follows we describe how our design was realized in practice and then discuss how our development performs in reducing handoff delay.

4.1 Implementation

Our proposal has been implemented over Linux Red Hat 9. We used Host AP[2] (Intersil's Prism 2/2.5/3 chipset) as the driver of wireless network interfaces that execute IEEE 802.1X functionality. Additionally, FreeRADIUS[3] and OpenSSL[4] were employed for secure message transfer between APs and the Authentication Server.

Location information exchanges are embodied in messages over the UDP/IP protocol stack. Fig. 6 (a) shows such message format comprising a header part and a collection of information entries, with fields defined below.

- *Code* indicates for what purpose the message is intended. A code value of 0, 1, and 2, respectively, represents the message to be used for Signal Report to some designated location server, request for prospective AP resolution, and reply containing a list of potential next APs for some concerned MS.
- *Entry Count* counts how many information entries are included in the message.
- *Timestamp* records the time instant when the message is sent.
- *Target AP Address* (layer-2 machine address) identifies a neighboring AP within the radio range of the MS.
- The remaining two fields, *Signal* and *Noise*, record the received signal strength and noise level of the target AP, respectively, by the MS. For a reply message to the MS, these two fields are filled with zeros.

We let MSs perform active scan, measure wireless link quality of APs within range, and then send Signal Reports to the location server. The location server will determine

[2] http://hostp.epitest.fi.
[3] http://www.freeradius.org.
[4] http://www.openssl.org.

potential next APs for an MS upon request. Figs. 6 (b)-(d) show example messages for these purposes.

The location server incorporates a daemon that is configured with AP-network topology of its administrative domain. The topology describes APs' coordinates and handoff-to relationship among APs provided by neighbor graphs. Once on, the daemon listens on a designated port for connection processing. The daemon records received Signal Reports from APs by MSs in storage. With this information in place, the daemon resolves on demand to which APs the MS is more likely to reassociate next. Generally we resolve more than one candidate AP for tolerating mobile direction uncertainty. Candidate APs are specified collectively in a reply message in the form of Fig. 6 (d) that will be sent to the requesting MS.

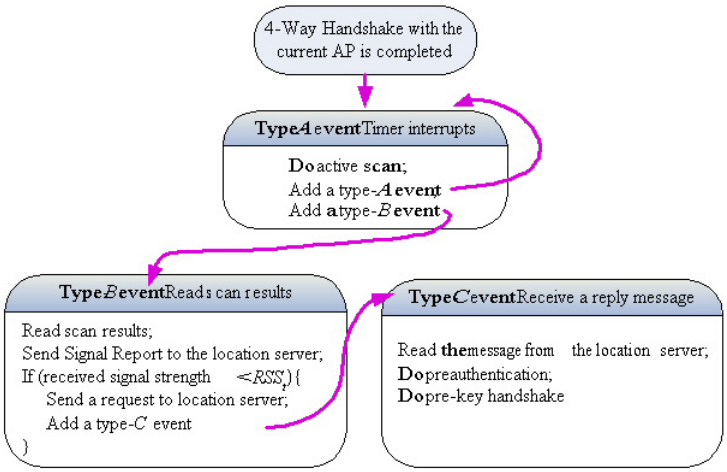


Fig. 7. A diagram of event handling at mobile client sides. The handling process involves three types of events.

Regarding mobile clients, we modified Host AP and its accompanied tool wpa_supplicant to support IEEE 802.11i network operations and interactions with the location server. In Host AP, each event is associated with a call-back function. A proper call-back function is invoked whenever a certain event occurs. As illustrated in Fig. 7, event handling at MS sides is described below.

- As the MS has completed a 4-Way Handshake with its current AP, the MS is able to proceed to data packets delivery. At this point, an event of type *A* is added by itself in its system space. A type-*A* event triggers a call-back function that sets a timer to schedule an active scan.
- When a type-*A* event occurs, the MS performs active scan, resets the timer for the next scan (type-*A* event), and then adds another event of type *B*. A type-*B* event triggers a call-back function that processes scan results.
- When a type-*B* event occurs, the MS measures its received signal strength and noise level from neighboring APs. These measures are sent as part of a Signal Report message to the location server. If the signal strength from the local AP has dropped below RSS_t,

the MS sends a request message to the location server for prospective AP resolution, and adds an event of type *C*. A type-*C* event triggers a call-back function that processes a reply message from the location server.
- When a type-*C* event occurs, the MS extracts information about its potential next AP(s) from the reply message. Subsequently the MS performs preauthentication and pre-handshake with each of indicated APs.

We extended the existing Robust Security Network (RSN) information element present in Beacon, Probe Response, or in (Re)Association Request frames. The information element is augmented to accommodate PTKID and pre-handshake capabilities, in following lines.

- We propose to append a 16-byte field termed *PTKID*. The field is optional though. The presence of this field means that the sending MS provides PTKID resulting from the completion of a pre-handshake. PTKID identifies a pairwise transient key for potentially immediate use by both the MS and local AP.
- We add a flag out of the original *Reserved* subfield of *RSN Capabilities*. The flag is referred to as *Pre-Handshakable* in this text, indicating whether or not the sending AP supports pre-handshake capability.

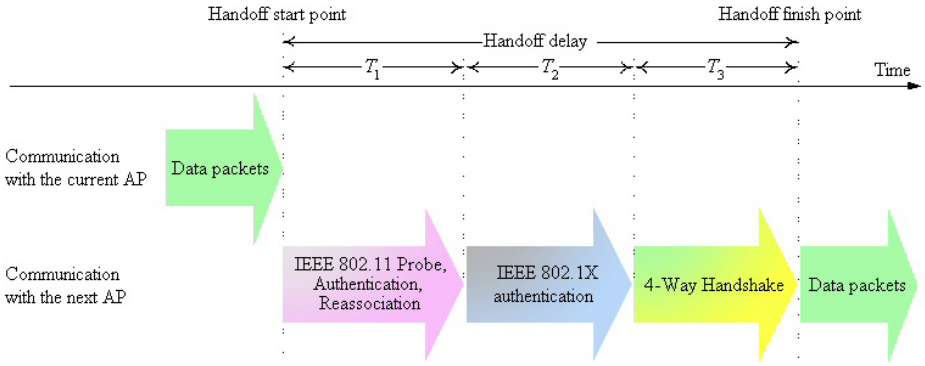
Other fields of the information element have the same meaning as with the original IEEE 802.11i specification. For definitions of these remaining fields, we refer the reader to [3].

4.2 Performance

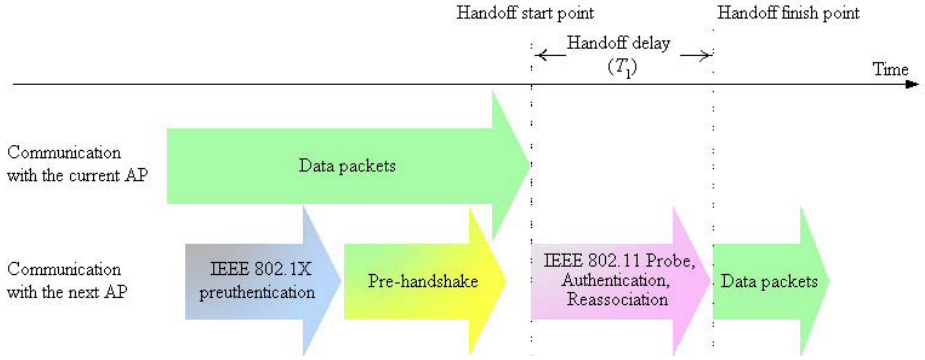
Concerning handoff delay, Fig. 8 (a) depicts a time diagram of a conventional handoff process. From the figure it can be seen that originally an MS maintains communication with its local AP. As the MS decides to switch its association over to another AP, data packets are held from being transported for a period. During the period, the MS relocates a new AP (taking T_1 time units), performs IEEE 802.1X authentication (taking a delay of T_2), and then carries out a 4-Way Handshake (incurring a delay of T_3). Afterward data packets delivery is resumed. Therefore handoff delay amounts to $T_1 + T_2 + T_3$. For fast handoff schemes using preauthentication, their handoff delay can be abridged to $T_1 + T_3$.

Fig. 8 (b) illustrates handoff delay in our architecture, where an MS completes preauthentication and pre-handshake procedures with a new AP prior to handoff. When the MS reassociates with the new AP locally, IEEE 802.1X authentication and 4-Way Handshake are bypassed. Subsequently the MS proceeds to normal data delivery straightway. Therefore our handoff delay is reduced to T_1. Given that delays for (re)association, IEEE 802.1X, and 4-Way Handshake average 2, 250, and 60 ms, respectively [6], our approach outperforms a conventional handoff scheme by 99% in terms of handoff delay. As compared with counterpart fast handoff schemes, our approach gains 96.8% outperformance in the same metrics, a marked improvement.

Observe that T_1, T_2, and T_3 vary on different platforms running different IEEE 802.1X authentication methods over diverse network topology. For instance, we conducted additional experiments in a simple environment shown in Fig. 9, composed of an



(a) A conventional handoff process.



(b) Our fast handoff process.

Fig. 8. Timing diagrams of different handoff schemes. (For convenience of illustration, Fig. (b) was not diagrammed in alignment with (a).)

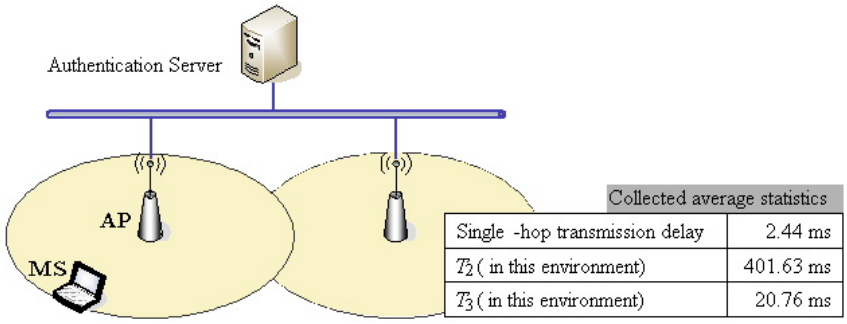


Fig. 9. Experimental environment.

Authentication Server, two APs, and an MS residing in a Local Area Network. The MS is a laptop PC running Windows XP SP2 with built-in Windows Zero Configuration Service. APs are two identical PCs running hostapd-0.5.7. The Authentication Server executes FreeRADIUS-1.1.4. The IEEE 802.11i encryption protocol in use is WPA2/AES and the authentication method is PEAP/EAP-MSCHAPv2. Repeating 20 identical ex-

periments gives average statistics: single-hop message transfer taking 2.44 ms, T_2 401.63 ms, and T_3 20.76 ms.[5]

Note that our scheme may lose its advantage when mispredicting the next potential AP or when handoff occurs before intended preauthentication and pre-handshake with the correct target AP have been completed. Either case is termed a *miss* here, implying that the MS shall undergo a conventional handoff process without gains from our design. To see how our scheme performs subject to misses, given reassociation, IEEE 802.1X, and 4-Way Handshake accounting for an average delay of 2, 250, and 60 ms, respectively [6], our approach incurs mean handoff latency

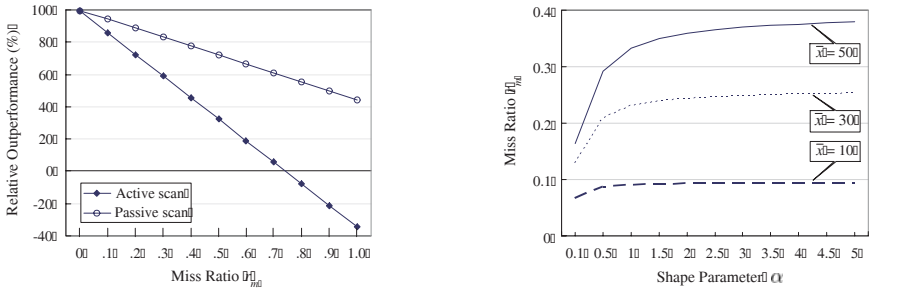
$$L = 2 + r_m \cdot (250 + 60), \tag{1}$$

where r_m denotes the miss ratio.

Concerning counterpart fast handoff schemes like [2, 14, 15], suppose that necessary security contexts are available on APs throughout, the best case where these schemes operate free from any miss (otherwise another factor analogous to r_m should be included). In this case the MS is able to reassociates to a new AP without going through IEEE 802.1X authentication. Still, AP discovery takes 0 to 1000 ms (active scan), or 40 to 300 ms (passive scan) [6], depending upon which scanning mode in use. Assuming that active and passive scanning cause a mean delay of (0 + 1000)/2 and (4 + 300)/2, respectively, these schemes operate with an average handoff latency

$$L' = \begin{cases} (0+1000)/2 + 2 + 60 & \text{active scan} \\ (40+300)/2 + 2 + 60 & \text{passive scan} \end{cases}. \tag{2}$$

Fig. 10 (a) relates our approach to counterpart schemes in terms of $(L' - L)/L'$ versus miss ratios. This figure indicates that our approach maintains appreciable improvement over counterpart schemes when $r_m \leq 0.7$. The condition of low r_m is arguably very probable to hold in practice, since roaming within IEEE 802.11-based networks like indoor



(a) Our performance gain relative to counterpart schemes using active or passive scan.

(b) Expected miss ratios under different network dynamics ($\overline{\tau}$ = 100 time units).

Fig. 10. Performance measures in our architecture.

[5] Based on these constituent statistics, system operational metrics of interest can be assessed by allowing for hop count or message complexity. For example, the product of the constituent T_2 and the average hop count between APs and the Authentication Server expresses an effective IEEE 802.1X delay in accord with real network topology. These metrics fit our developed evaluation model of section 4.

environment is in general not speedy. Hence sudden, early handoff would occur rarely. In this regard, for $r_m \leq 0.4$ as an example, our approach can save handoff delay by over 43%. Note that, however, Fig. 10 (a) also signifies when our approach may become ineffective in reducing handoff delay – when r_m grows too high. Both upside and downside along with their inclinations present in the figure give a fairer view of how our approach performs at large.

To see how small r_m takes on, let us consider the case where misses are mainly due to early handoff, leaving out insignificant target AP misprediction thanks to locality property and neighbor graph as reasoned in section 3.2. Let τ denote the elapsed time from the point when our advance operations are initiated to the point when the MS disassociates from its current AP. Assume that the residual time τ is exponentially distributed with probability density $\mu e^{-\mu\tau}$ and that the duration x of completing preauthentication and pre-handshake collectively over the network is gamma distributed with density $f(x) = \frac{1}{\Gamma(\alpha)\beta}(\frac{x}{\beta})^{\alpha-1}e^{-x/\beta}$. The gamma distribution is adopted here for its versatility of approximating general, stochastic behavior of random variables [9] to represent wide-ranging network dynamics. The versatility is due to the richness of the gamma function $\Gamma(\alpha)$; by varying the parameters α and β it is possible to fit the gamma distribution to many types of experimental data. For selecting proper α and β to our purpose, we can use $\alpha\beta$ and $\alpha\beta^2$ to match the mean and variance of x, respectively.

Recall that an early handoff results from time requirement x exceeding the MS's residual time τ. Accordingly the miss ratio r_m can be formulated as the probability of x longer than τ, so

$$r_m = Prob[\tau < x] = \int_0^\infty (\int_0^x \mu e^{-\mu\tau} d\tau) f(x) dx = 1 - (\frac{1}{1+\beta\mu})^\alpha. \quad (3)$$

Note that $(\frac{1}{1+\beta\mu})^\alpha$ above is exactly the Laplace transform of $f(x)$. Eq. (3) justifies a small value of r_m in that τ (pertinent to user movement speed) is typically at least one order of magnitude larger than x (relevant to network speed). To see this, for instance, considering τ with mean $\bar{\tau} = 1/\mu$ set to, say, 100 time units and x with mean $\bar{x} = \alpha\beta$ equal to 10, 30, and 50, respectively, Fig. 10 (b) plots the distribution of r_m on condition of different combinations of α and β. (For simplicity, these data were collected by varying the shape parameter α; once α is determined, the scale parameter β changes correspondingly for fixed $\bar{x}$.) The figure shows that r_m is kept asymptotically low throughout, even in a relatively extreme case of $\bar{x} = 50$ versus $\bar{\tau} = 100$ where the magnitude disparity between x and τ is not evident.

Note an issue that may arise when an MS performs our protocol, taking up some air time for data traffic delivery. This happens if the MS is equipped with a half-duplex transceiver, bringing about potential throughput degradation. Indeed, the issue is common to IEEE 802.11i-conformant secure fast handoff schemes, because the required IEEE 802.1X operations involve the MS. The adverse effect on throughput hinges upon data traffic patterns and is in general arguably immaterial. This is because data traffic often takes on an ON-OFF pattern, except for constant-bit rate traffic. It is thus suggested that our protocol be executed when there is no ongoing data burst detected. By doing so, network throughput is maintained without loss. In addition, since our protocol produces merely short, small quantities of messages, our bandwidth usage is insignificant as com-

pared with that for potentially long-lasting data sessions, even though our protocol messages are interleaved in constant-bit rate traffic.

5. CONCLUSIONS

The small coverage of IEEE 802.11 networks may lead mobile users to suffer frequent handoffs among APs of different mobility domains. The provision of secure fast handoff in such network settings is essential, since conventional IEEE 802.11r does not allow for inter-domain mobility. In view of this issue, we availed ourselves of IEEE 802.11i standard mechanisms and presented treatment in two main aspects: pre-handshake (subsequent to preauthentication) and the introduction of a location server. The former aspect lets an MS preauthenticate and establish a cryptographic key with target APs before handoff. The established key is then kept in a designated data structure for quick matching. The latter is to facilitate the MS to learn about its potential next APs in a more judicious fashion. The location server aware of the station's movement tendency assesses with which AP(s) the MS is likely to reassociate next. This enables the MS to preauthenticate to few APs, but not to a broader set of neighboring APs than necessary. We have also implemented our approach on a Linux platform. Performance discussions indicate that our proposal is effective in practice. It is apropos to apply our approach as a complement to the emerging IEEE 802.11r standard.

To conclude this paper, we remark that our design elegantly lends itself to an ingredient of cross-layer fast handoff schemes as well. Cross-layer fast handoff deals with the case where link level events are used to assist triggering network level handoff of a roaming station that needs to acquire new IP addresses along its migration. The development of such techniques, an active research area, benefits users moving across administrative domains (macro mobility).

REFERENCES

1. IEEE Std 802.11, 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, 1999.
2. IEEE 802.11F, Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation, 2003.
3. IEEE Std 802.11i, IEEE Standard for Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements – Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Medium Access Control (MAC) Security Enhancements, 2004.
4. IEEE Std 802.11r, 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; Amendament 2: Fast Basic Service Set (BSS) Transition, 2008.

5. IEEE 802.21, Standard for Local and Metropolitan Area Networks – Part 21: Media Independent Handover Services, 2009.
6. B. Aboba, *Fast Handoff Issues*, IEEE-03-155r0-I, IEEE 802.11 Working Group, 2003.
7. B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible authentication protocol (EAP)," RFC 3748, IETF Network Working Group, 2004.
8. K. H. Chi, J. H. Jiang, and L. H. Yen, "Cost-effective caching for mobility support in IEEE 802.1X frameworks," *IEEE Transactions on Mobile Computing*, Vol. 5, 2006, pp. 1547-1560.
9. A. Leon-Garcia, *Probability and Random Processes for Electrical Engineering*, 2nd ed., Addison-Wesley Publishing Company, Inc., Massachusetts, 1994.
10. A. Mishra, M. H. Shin, and W. Arbaugh, "Context caching using neighbor graphs for fast handoffs in a wireless network," in *Proceedings of the 23rd IEEE Conference on Computer Communications*, 2004, pp. 351-361.
11. A. Mishra, M. H. Shin, N. L. Petroni, Jr., T. C. Clancy, and W. A. Arbaugh, "Proactive key distribution using neighbor graphs," *IEEE Wireless Communications*, Vol. 11, 2004, pp. 26-36.
12. IEEE P802.1X/D11, Standards for Local Area and Metropolitan Area Networks: Standard for Port Based Network Access Control, 2001.
13. S. Pack, J. Choi, T. Kwon, and Y. Choi, "Fast handoff support in IEEE 802.11 wireless networks," *IEEE Communications Surveys and Tutorials*, Vol. 9, 2007, pp. 2-12.
14. S. Pack and Y. Choi, "Fast inter-AP handoff using predictive authentication scheme in a public wireless LAN," in *Proceedings of IEEE Networks*, 2002, pp. 15-26.
15. S. Pack and Y. Choi, "Pre-authenticated fast handoff in a public wireless LAN based on IEEE 802.1X model," in *Proceedings of Personal Wireless Communications*, 2002, pp. 175-182.
16. S. Pack, H. Jung, T. Kwon, and Y. Choi, "SNC: A selective neighbor caching scheme for fast handoff in IEEE 802.11 wireless networks," *ACM Mobile Computing and Communications Review*, Vol. 9, 2005, pp. 39-49.
17. K. Pahlavan, X. Li, and J. P. Makela, "Indoor geolocation science and technology," *IEEE Communications Magazine*, Vol. 40, 2002, pp. 112-118.
18. C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote authentication dial in user service (RADIUS)," RFC 2865, IETF Network Working Group, 2000.
19. C. C. Tseng, K. H. Chi, M. D. Hsieh, and H. H. Chang, "Location-based fast handoff for IEEE 802.11 networks," *IEEE Communications Letters*, Vol. 9, 2005, pp. 304-306.

Kuang-Hui Chi (紀光輝) was Assistant Professor (2003-2009) and is currently Associate Professor at the Department of Electrical Engineering, National Yunlin University of Science and Technology, Taiwan. He received his B.S. degree in Computer Science and Engineering, Tatung University in 1991. He earned M.S. (1993) and Ph.D. (2001) degrees in Computer Science and Information Engineering, both from National Chiao Tung University. From 2001 to 2003, he was with Computer and

Communications Research Laboratories, Industrial Technology Research Institute, R.O.C. His current research interests include wireless internet and protocol verification.

Chien-Chao Tseng (曾建超) is currently a professor in the Department of Computer Science at National Chiao Tung University, Hsinchu, Taiwan. He received his B.S. degree in Industrial Engineering from National Tsing Hua University, Hsinchu, Taiwan, in 1981; M.S. and Ph.D. degrees in Computer Science from the Southern Methodist University, Dallas, Texas, USA, in 1986 and 1989, respectively. His research interests include wireless internet, handover techniques for heterogeneous networks, and mobile computing.

Ya-Hsuan Tsai (蔡亞軒) is currently a software engineer at Trend Micro, an internationally renowned company offering security solutions that protect against a wide range of insidious threats and many varieties of combined attacks. He received his B.S. and M.S. degrees in Computer Science and Information Engineering from National Chiao Tung University in 2003 and 2005, respectively. His current research interests include kernel programming and file system filter drivers.