Fast Handoff in Secure IEEE 802.11s Mesh Networks

Kuang-Hui Chi, *Member, IEEE*, Yung-Chien Shih, Ho-Han Liu, Jui-Tang Wang, Shiao-Li (Charles) Tsao, *Member, IEEE*, and Chien-Chao Tseng

***Abstract*—While mesh networking is gaining momentum with widespread application, we are concerned with fast handoff in a secure mesh environment. To this end, this paper presents a means in the context of IEEE 802.11s of letting a mesh portal act as an IEEE 802.1X authenticator to reduce costly IEEE 802.1X authentication processes during handoff. Our approach is developed for alignment with IEEE 802.11s and 802.11i, keeping protocols at the station side operable with no changes. As another strength, our design applies to generic multihop wireless networks. Both analytical and simulation modeling are conducted to evaluate our scheme as well. Performance results show that our approach reduces handoff delay by up to 268% or achieves comparable performance resulting from the counterpart IEEE 802.11i scheme with high likelihood of 70%–85% successful preauthentication. Moreover, our performance analysis suggests an optimal number of access points managed by one mesh portal in a network. Qualitative and quantitative discussions indicate that our approach is applicable in pragmatic settings.**

***Index Terms*—Fast handoff, IEEE 802.11i, IEEE 802.11s, mesh network, random walk model, security domain.**

I. Introduction

IEEE 802.11s specifies how IEEE 802.11 devices are interconnected for mesh networking [3], [8], [13]. A wireless mesh network does not necessitate cabling, as opposed to a typical architecture where stations communicate via access points (APs) attached to a wired medium. This new type of network architecture facilitates rapid deployment and is evolving as a vital means of public access to the Internet services.

A handoff process occurs when a station moves its association from one AP to another, causing a blackout period of communication disruption. Handoff involves AP discovery, authentication, reassociation establishment, and inter-AP transfer of physical connectivity or credential information specific to the mobile station. AP discovery by the station identifies APs within range. The authentication procedure refers to legacy open-system and IEEE 802.1X authentication processes [9]. For user authentication and keying material distribution, the IEEE 802.1X framework has been adopted as a mandatory part of Robust Security Networks (IEEE 802.11i [11]). With IEEE 802.1X transactions at a remote site, internetwork operations account for another potentially prohibitive delay. As far as secure communication is concerned, however, we should avail ourselves of IEEE 802.11i mechanisms to the greatest extent possible.

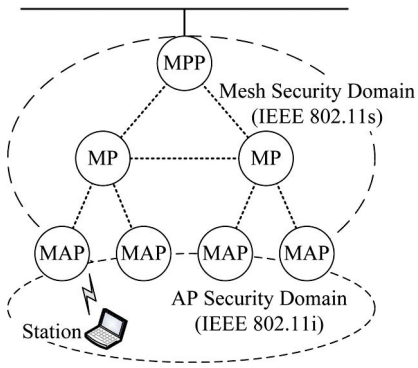

Fig. 1. Mesh networking security architecture.

This paper deals with roaming in an IEEE 802.11 mesh network while maintaining secure communication, as per IEEE 802.11i. As shown in Fig. 1, a mesh network comprises a mesh security domain and AP security domains. A security domain refers to a set of network entities on which a same security policy is exercised under a single administrative authority [23]. The mesh security domain covers mesh points (MPs) connecting to a mesh portal (MPP), whereas an AP security domain encompasses a mesh AP (MAP) and its local stations. (A MAP is an MP providing additional AP functionality.) Observe that current policies adopted in these security domains are different; links among MPs are protected by IEEE 802.11s, whereas connectivity between a station and its local MAP is protected by IEEE 802.11i mechanisms.

Whenever a mobile station switches its association to a new MAP, IEEE 802.1X requires the station and an Authentication Server situated its home network to authenticate each other. IEEE 802.1X authentication involves mostly multiple rounds of message exchanges through the Internet, at the expense of nontrivial delay. For this, a number of fast handoff schemes have been developed, e.g., [9], [17]–[20], [22], and [24] (see [21] for an expository survey). However, these schemes did not take mesh infrastructure into account. As a remedy, we

Manuscript received September 8, 2008; revised June 11, 2010 and August 6, 2010; accepted October 1, 2010. Date of publication October 28, 2010; date of current version January 20, 2011. This work was supported by the National Science Council under Grant NSC 97-2221-E-009-051-MY3, Grant NSC 99-2220-E-009-046, and Grant 7352B41100. The review of this paper was coordinated by Dr. L. Chen.

K.-H. Chi is with the Department of Electrical Engineering, National Yunlin University of Science and Technology, Touliu 640, Taiwan (e-mail: chikh@yuntech.edu.tw).

Y.-C. Shih is with the Institute of Computer Science and Engineering, National Chiao Tung University, Hsinchu 300, Taiwan, and also with Telcordia Applied Research Center Taiwan Company, Taipei 115, Taiwan (e-mail: ycshih@csie.nctu.edu.tw).

H.-H. Liu, S.-L. Tsao, and C.-C. Tseng (Corresponding author) are with the Institute of Computer Science and Engineering, National Chiao Tung University, Hsinchu 300, Taiwan (e-mail: hohanliu@gmail.com; sltsao@csie.nctu.edu.tw; cctseng@csie.nctu.edu.tw).

J.-T. Wang was with the Institute of Computer Science and Engineering, National Chiao Tung University, Hsinchu 300, Taiwan. He is now with the Information and Communications Research Laboratories, Industrial Technology Research Institute, Hsinchu 310, Taiwan (e-mail: rtwang@csie.nctu.edu.tw).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2010.2090050

0018-9545/$26.00 © 2010 IEEE

propose an avenue to streamline secure communication in a wireless mesh network despite handoff. Our proposed scheme distinguishes itself from previous work in several aspects.

1) The security level in line with IEEE 802.11i is well maintained, without compromising required robust security.
2) We avoid distributing sensitive keying material, i.e., pairwise master keys (PMKs; see Section II-A), over the wireless medium and thereby rule out undue access from the air.
3) IEEE 802.1X authentication can be bypassed during handoff to reduce overall delay in a way that moderate network size is suggested.
4) Current protocols at the station side remain operable with no changes, allowing backward and forward compatibility.
5) Our approach is interoperable with the emerging IEEE 802.11s standard, indicating its usefulness in practical application.
6) Our design elegantly lends itself to generic multihop wireless networks, in particular clustered networks accommodating IEEE 802.1X.

Indeed, our approach is complementary to, but not competing with, IEEE 802.11s-based schemes nor is it developed in place of the ritual of IEEE 802.11s. In our architecture, an alternative end-to-end secure communication channel between a mobile station and its MPP is ensured such that repeated encryptions and decryptions in frame delivery can be substantially saved. We stress that authentication processes and secure messaging for mobile stations are of concern to this paper, but otherwise, we exploit IEEE 802.11s mechanisms such as MP authentication or secure transfer of signaling messages in the mesh infrastructure where available.

The remainder of this paper is organized as follows: The next section gives a brief background on this study. Section III describes our proposed scheme, including system architecture, message flows, and security analysis. Performance evaluation is provided in Section IV. Finally, Section V concludes this paper.

II. Background

As shown in Fig. 1, an IEEE 802.11 mesh network is composed of MPs that are interconnected via wireless links. MPs form mesh links over which mesh paths are established using a routing protocol. An MP providing both mesh services and AP functionality is referred to as a MAP. A mobile station (or a station for short) needs to associate with a MAP for network access. In practice, the network generally contains a number of AP security domains and a mesh security domain.

A. Security Association

A security association refers to the establishment of shared security information such as credentials or cryptographic keys between two network entities to support secure communication. Within an AP security domain, IEEE 802.11i mechanisms, namely, IEEE 802.1X authentication, four-way handshake, and encryption protocols (Temporal Key Integrity Protocol or Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), are used. These mechanisms are collectively meant to establish a security association between a station and its MAP.

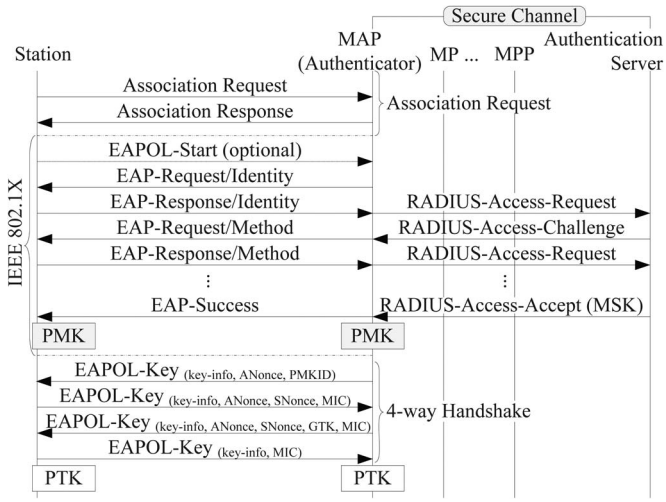

Fig. 2. Message flow to and from an AP security domain.

For access control, as shown in Fig. 2, IEEE 802.1X authentication starts with an Extensible Authentication Protocol over LAN (EAPOL)-Start frame by the supplicant station or an Extensible Authentication Protocol (EAP)-Request/Identity packet by the associated MAP. In response, the station provides its identity using an EAP-Response/Identity packet, which is then encapsulated in a RADIUS-Access-Request message addressed to the backend Authentication Server. The following are challenge–response interactions between the station and the Authentication Server in several round-trips, depending on what EAP method is in use [1]. After such EAP interactions have successfully terminated, these two parties generate a common master session key (MSK) for authorization purposes. The Authentication Server then sends the MSK to the serving MAP in a RADIUS-Access-Accept packet for authorization. Upon reception, the IEEE 802.1X authentication process is completed when an EAP-Success packet is generated toward the supplicant station, whereby a PMK is derived, as stipulated by IEEE 802.11i.

After successful IEEE 802.1X authentication, four-way handshake takes place (see Fig. 2). This procedure involving four EAPOL-Key frames is used by both the station and its local MAP to confirm the possession of a correct PMK and to derive a pairwise transient key (PTK). Four-way handshake is initiated by the MAP sending the first EAPOL-Key frame to the station, containing a randomly chosen number ANonce and a PMK identifier (PMKID) indicative of which PMK shall be used. Then, the station derives a fresh PTK and sends back a frame containing SNonce (which is another random number selected by the station), certain information elements, and a message integrity code (MIC). Subsequently, the MAP derives a PTK identical to that on the station side and checks the integrity of the received frame. If valid, the MAP acknowledges the station using the third EAPOL-Key frame that may include a group temporal key (GTK). Finally, the station responds to the MAP using the fourth frame to terminate the handshake, whereupon a security association is established between these two sides.

Apart from IEEE 802.11i, IEEE 802.11s defines efficient mesh security association (EMSA) [13], involving EMSA authentication, four-way handshake, key distribution, and encryption protocols. While the IEEE 802.1X framework is still adopted, an MP can act both as a supplicant and an authenticator. Each MP authenticates its neighboring MP, establishes a PTK, and sends a GTK through key distribution and authentication processes. It is noted that key distribution includes the delivery of PMKs for mesh authenticators, which are termed PMK-MAs, from some mesh key distributors. Based on a PMK-MA, an authenticator MP and its supplicant MP mutually derive a PTK. EMSA allows multiple MPs to instantiate a security association without invoking IEEE 802.1X authentication. In this paper, EMSA is honored. We aim to augment AP security domains so that our development can cooperate additionally with well-defined mechanisms such as EMSA in the mesh security domain.

B. Standard Fast Handoff Mechanisms

As stated, a handoff process involves AP discovery, commit phase (legacy open-system authentication and reassociation), IEEE 802.1X authentication, and four-way handshake. Among others, the study in [5] indicates that IEEE 802.1X authentication accounts for most handoff delay (75%–95%). In view of this major determinant, we shall leverage an IEEE 802.11i preauthentication mechanism to let a station perform IEEE 802.1X authentication with a target AP beforehand. Essentially, such preauthentication operates in the same way as the IEEE 802.1X authentication that was prescribed in Section II-A, except that all EAPOL frames are forwarded via the station's current MAP as an intermediary. After successful preauthentication, a newly derived PMK is cached at the station and the target MAP for future use. When reassociating with the target MAP later, the station provides a PMKID in its Association Request frame to signify that a corresponding PMK has been cached. If the provided PMKID is valid, the target MAP can save itself IEEE 802.1X authentication and carry out four-way handshake straightaway.

We remark that IEEE 802.11r is another emerging standard specifying mechanism to speed up transitions of a station among APs within a *mobility domain*, which is a managed set of APs sharing security associations [12]. IEEE 802.11r optimizes message exchanges and separates IEEE 802.1X authentication from network access control during each handoff. However, a means of target AP prediction is required somehow. For backward compatibility with a vast set of end-user equipment, we propose an alternative approach to secure fast handoff in mesh networks.[1] Neither an MSK nor a PMK is transmitted over wireless media. In alignment with standard IEEE 802.11 machinery, our approach keeps current protocols at the station side operable without change, as shall be seen next.

[1]A number of studies have shown that target AP-prediction techniques are of use to reduce handoff delay. Such techniques can be programmed in IEEE 802.11 devices via firmware updates or controlled by user space software. In comparison, we take another avenue to achieve similar objectives by restructuring the IEEE 802.1X framework, making our scheme transparent to end users and independent of AP prediction. However, our scheme can combine with target AP prediction techniques to secure fast handoff support. Our scheme is indeed complementary to these techniques.

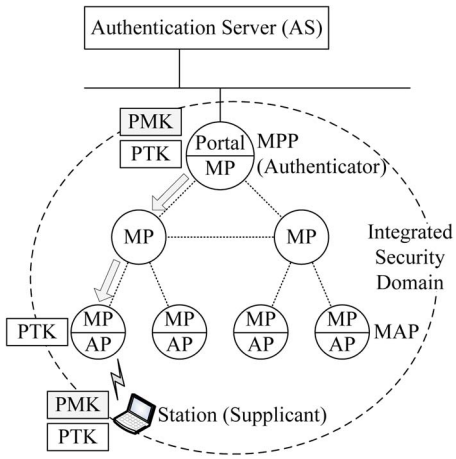

Fig. 3. Extending AP security domains to a mesh network environment.

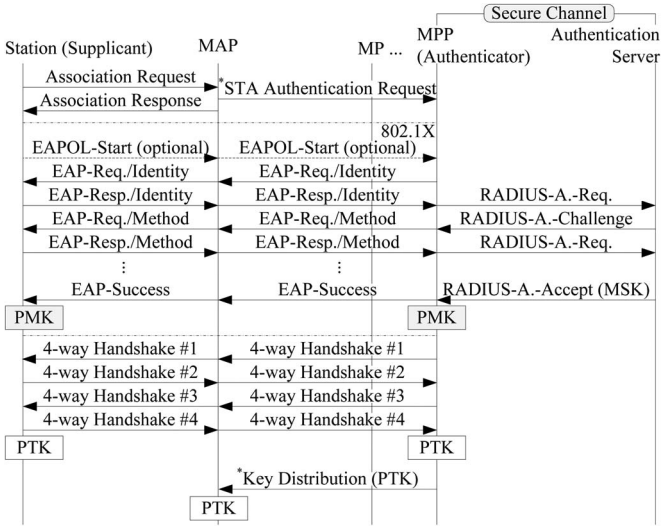

Fig. 4. Message flow of establishing a security association in our architecture. Messages marked with "*" represent our addenda.

III. Proposed Approach

We extend AP security domains to a mesh network (see Fig. 3) to reduce repeated IEEE 802.1X authentication and encryption/decryption processing of data frames for mobile stations. In our architecture, a station performs IEEE 802.1X authentication only when (re)associated with a MAP in the network for the first time. The role of an authenticator is now shifted from a MAP to an MPP. As an MPP partakes in IEEE 802.1X authentication and cryptographic key management, we maintain an end-to-end secure channel between the station and the MPP wherever the station roams in the network. MAPs at the edge of a mesh network remain responsible for blocking unauthenticated stations from access to the system. To enable a MAP to verify frame integrity, a PTK and a GTK are distributed from the MPP to the serving MAP via secure mesh links immediately after four-way handshake (see also Fig. 4).

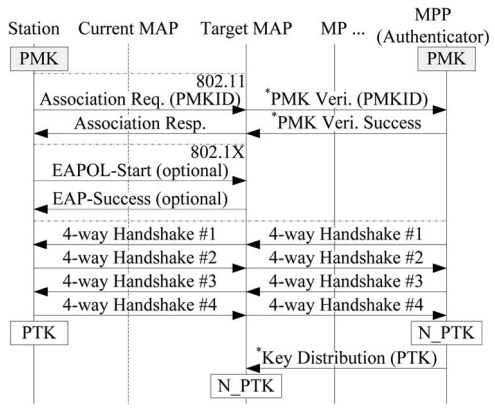

Fig. 5. Intra-MPP handoff message flow without the involvement of any IEEE 802.1X Authentication Server.

A. Security Association Establishment

When a station is initially (re)associated with any MAP managed by an MPP, it performs IEEE 802.1X authentication and four-way handshake to create the security association with the MPP as per IEEE 802.11i. In our architecture, however, since the MPP is *de facto* an authenticator, the serving MAP acts as a transit node that forwards IEEE 802.1X traffic between the station and the MPP, as depicted in Fig. 4 in the following lines.

1) The serving MAP examines whether a valid PMKID is included in the (Re)Association Request frame by the station. If not, we let the MAP generate a designated message, which is named STA Authentication Request, toward the MPP to initiate IEEE 802.1X authentication.
2) The station proceeds to IEEE 802.1X authentication and four-way handshake with the MPP via the serving MAP.
3) Then, the MPP uses a Key Distribution message to inform the serving MAP of the newly derived PTK. A GTK assigned by the MPP, if any, in four-way handshake can also be included in the same message meant for the MAP.
4) Upon receipt of the PTK, the serving MAP allows the station to access the network hereinafter.

B. Handoff Procedure

Handoff occurs when a mobile station reassociates from one MAP to another, in two possible cases, namely, intra-MPP and inter-MPP handoff. The former means that the station reassociates with another MAP connected to the same MPP. Since the IEEE 802.1X authenticator (MPP) remains unchanged, PMKs cached on the station and the MPP sides serve as a basis for mutual authentication, leaving out IEEE 802.1X authentication. Fig. 5 shows the message flow of such an intra-MPP handoff procedure.

1) The reassociating station sends a PMKID to its target MAP, which then forwards a PMKID to the MPP to validate the cached PMK on the station side.
2) The PMKID is used to identify the PMK cached in the MPP. If the PMKID is found valid, the MPP notifies the target MAP using a PMK Verification Success message.

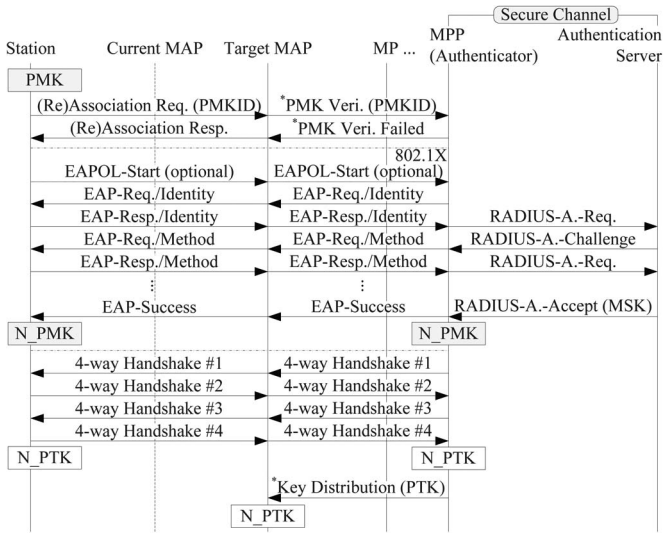

Fig. 6. Inter-MPP handoff message flow.

3) Upon receiving an EAPOL-Start frame, the target MAP replies an EAP-Success message directly, with no need to contact the backend Authentication Server.
4) Then, four-way handshake and PTK distribution follow, as shown in Section III-A.

On the other hand, inter-MPP handoff takes place when a station moves across MAPs managed by different MPPs. In this case, the station performs IEEE 802.1X preauthentication with its new target MPP (see Fig. 6), unless the station has retained a correct PMK for the newly visited domain. A message flow is described here.

1) The station reassociates with the target MAP. The PMKID included in the (Re)Association Request frame is forwarded by the receiving MAP to the new MPP to validate the cached PMK, if any.
2) Provided that the new MPP cannot find the corresponding PMK, a message (PMK Verification Failure) is sent to the target MAP to trigger IEEE 802.1X authentication for the station.
3) Accordingly, IEEE 802.1X authentication and four-way handshake are activated and then followed by PTK distribution. These procedures operate as prescribed in Section III-A.

It is noted that IEEE 802.1X authentication delay remains present if preauthentication fails for some reason.

C. Frame Delivery

In our architecture, we establish an end-to-end secure channel between each station and its MPP. Therefore, in the event of communication with a correspondent host outside the mesh network, only a station's serving a MAP and an MPP are required to encrypt/decrypt frames. This can be accomplished by extending the use of IEEE 802.11i encryption protocols to the entire mesh network while preventing the MAC header from being altered. In practice, we introduce a bidirectional MAC tunnel between serving a MAP and an MPP. Fig. 7(a) gives an example of our encapsulation process.

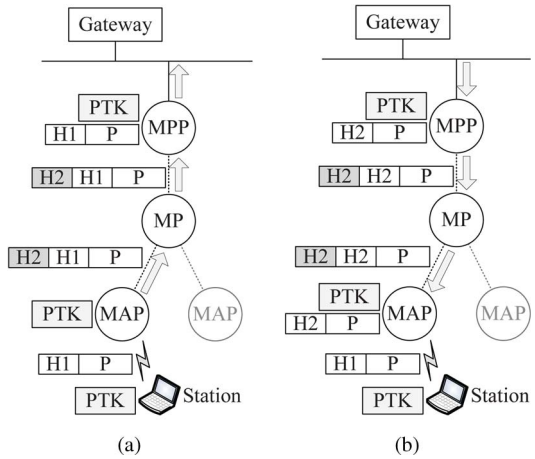

Fig. 7. Frame delivery involving bidirectional MAC tunneling. (a) Outbound frame. (b) Incoming frame.

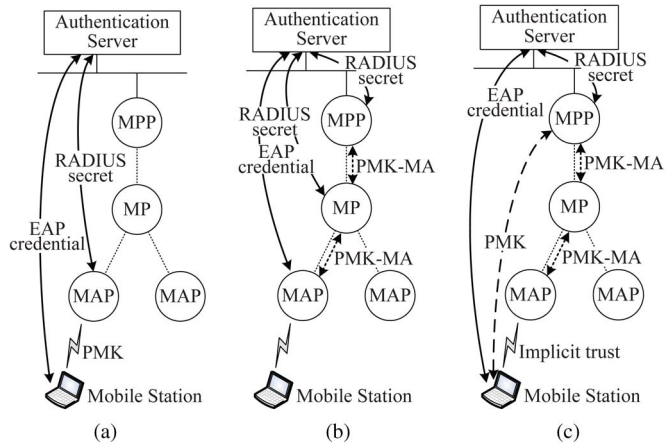

Fig. 8. Trust relationships in different network paradigms. (a) IEEE 802.11i. (b) IEEE 802.11s. (c) Our architecture.

Supposing that a station communicates with a node outside the mesh network, frame delivery takes three steps.

1) The station prepares an outgoing frame of the form $\langle \mathrm{H1}, \mathrm{P} \rangle$, where H1 and P denote the frame header and the payload, respectively. The frame is encrypted using the station's PTK and then transmitted to the serving MAP.
2) The serving MAP verifies the MIC of the received frame using the PTK. A frame with a correct MIC is further processed or discarded otherwise. If the destination site is found outside the mesh network, the MAP encapsulates the frame in a form $\langle \mathrm{H2}, \mathrm{H1}, \mathrm{P} \rangle$, where H2 is the MAC header meant for IEEE 802.11s routing. The encapsulated frame is then forwarded hop by hop toward the MPP. Note that the outer header may be replaced anew at intermediate MPs for next-hop forwarding, whereas the inner header (H1) is kept unchanged throughout the routing process.
3) Upon receipt, the MPP removes the outer header (H2) and decrypts the inner frame $\langle \mathrm{H1}, \mathrm{P} \rangle$ using the corresponding PTK. Subsequently, the MPP encapsulates the payload (P) into an Ethernet frame and forwards the frame to the destination.

In contrast, Fig. 7(b) illustrates a scenario where a node outside the mesh network sends a data frame to a mobile station. The inbound delivery is given here.

1) The MPP translates the received frame (from the gateway) into an IEEE 802.11 format of the form $\langle \mathrm{H2}, \mathrm{P} \rangle$. The frame is encrypted using the corresponding PTK, encapsulated in a form $\langle \mathrm{H2}, \mathrm{H2}, \mathrm{P} \rangle$, and then forwarded hop by hop toward the destination station. Here, two identical MAC headers are used to keep the inner header intact during routing within the mesh network.
2) When the frame arrives at the local MAP of the intended station, the outer header is removed, and the resulting inner frame is decrypted using the PTK.
3) The MAP encapsulates the decrypted payload (P) into an IEEE 802.11 frame $\langle \mathrm{H1}, \mathrm{P} \rangle$ and encrypts the resulting frame using the PTK again. Then, the MAP forwards the frame to the station.

In the case that both source and destination nodes are located in the same mesh network, the IEEE 802.11s shortcut routing [13] technique applies.

Note that our bidirectional MAC tunneling mechanism is not part of IEEE 802.11s, but similar methodology appeared in some contexts, such as Virtual Private LAN Service [15] or IEEE 802.1ah bridge protocols. The frame size limit on our MAC tunneling is the maximum allowed frame size in IEEE 802.11s (1552 bytes) minus the length of the IEEE 802.11s frame header, as the extra header we use for encapsulation is of the IEEE 802.11s-specified format. To prevent fragmentation due to exceeding the maximum transmission unit a link-layer protocol can carry, the mesh network can be configured by setting the maximum transmission unit to 1552 bytes accordingly.

D. Security Considerations

We argue that, in our architecture, wireless communication between each station and its MAP remains secure and that our achieved security level is no weaker than IEEE 802.11i. Recall that stations and MAPs under discussion are IEEE 802.11i capable. In addition, mesh links among MPs have been protected by EMSA. In what follows, we reason about trust relationships and then discuss threat models.

1) Trust Relationships: In IEEE 802.11i, a station and its serving MAP perform IEEE 802.1X authentication and four-way handshake to establish a security association [based on the PMK, as shown in Fig. 8(a)], with a station–MAP trust relationship. The relationship results from two security associations: 1) between the mobile station and the Authentication Server (abbreviated to MS↔AS relationship), as ensured by EAP credentials; and 2) between the Authentication Server and the MAP (AS↔MAP relationship) by the RADIUS secret. Therefore, IEEE 802.11i implies an MS ↔ AS ↔ MAP trust chain.

To secure communication between the station and its MAP, our proposed solution should be proved to attain an equivalent station–MAP trust relationship. To see this, recollect that mesh links between two MPs are protected by EMSA (a PMK-MA ensures a MAP↔MP trust relationship), as indicated in

Fig. 8(b). Furthermore, a MAP, an MP, and the MPP maintain security associations with the Authentication Server using their respective RADIUS secrets (these MAPs and MPs are also using EAP credentials). Coalescing these relations gives a MAP $\leftrightarrow$ AS $\leftrightarrow$ MP $\leftrightarrow$ AS $\leftrightarrow \cdots \leftrightarrow$ MPP trust chain in the mesh security domain.

In our approach, as shown in Fig. 8(c), the station performs IEEE 802.1X authentication and four-way handshake with the MPP, forming an MS $\leftrightarrow$ AS $\leftrightarrow$ MPP trust chain. In addition, since there is a MAP$\leftrightarrow$MPP trust relationship resulting from PMK-MAs within the mesh security domain, the MS $\leftrightarrow$ MPP $\leftrightarrow$ MAP trust chain can be deduced from the former two trust relationships. Therefore, we assure that our architecture of the station–MAP trust relationship is equivalent to that in IEEE 802.11i.

2) Threat Models: To validate that our development maintains the due network security, we identify and discuss potential threats against our proposed mechanism.

1) *PMKID leakage:* Even if an attacker may learn the corresponding PMKID from previous eavesdropping and be able to skip IEEE 802.1X authentication, this does not cause a security flaw, impairing our architecture. This is because an MSK or any form of preshared keys is never transmitted over the wireless media, and thus, a valid PTK cannot be derived by the attacker. As a consequence, the attacker cannot compute the correct MIC of the second EAPOL-Key frame in four-way handshake; thus, the attacker is blocked by the MAP right away.
2) *Unauthorized disclosure:* Compromised mesh links may result in unauthorized disclosure of keying materials. For IEEE 802.11i, an MSK is transmitted from the Authentication Server to the serving MAP through mesh links. If mesh links are compromised, the MSK is possibly divulged to an attacker. As opposed to transmitting an MSK, our proposal transfers only a PTK via mesh links. Since the PTK takes a lower level than the MSK in key hierarchy, the exposed PTK accounts for less security degradation compared with the compromised MSK.
3) *Compromise of authenticators:* When an authenticator is compromised or stolen, an attacker may obtain all the PMKs cached in that authenticator. In this scenario, the attacker can access the mesh network via any MAP connected to that authenticator. However, such vulnerability is recognized reluctantly acceptable in IEEE 802.11 working groups. For example, IEEE 802.11r is also susceptible to the situation where a compromised authenticator may expose PMK-R0s to the attacker. Since IEEE 802.11 working groups permit this situation, we believe that the potential vulnerability is acceptable.

The aforementioned qualitative analysis shores up security aspects of our architecture. Next, we proceed to quantitative analysis of the proposed protocol.

IV. Performance Discussion

This section compares our fast handoff approach with the best known IEEE 802.11i scheme in terms of handoff delay and the amount of signaling traffic introduced by a handoff process. Our performance evaluation is conducted by means of analytical modeling and simulation modeling.

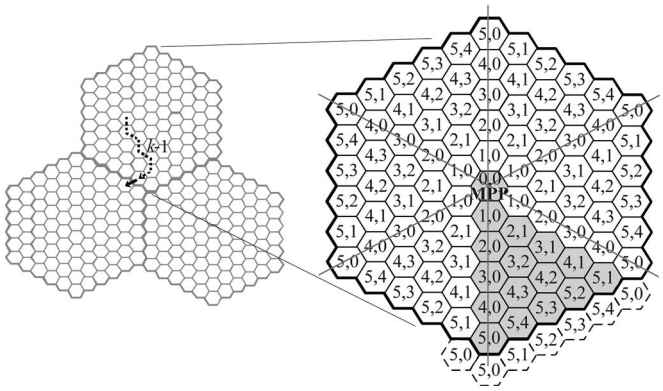

Fig. 9. Mesh network is viewed to consist of regions of cells, each region being served by an MPP. Every cell represents the radio coverage of a MAP, an MP, or an MPP.

A. Analytical Model

Our performance analysis is inspired from a clustering technique by Akyildiz *et al.* [4] that simplifies 2-D random walks over hexagonal and mesh planes to a reduced set of cells. As in that study, Fig. 9 illustrates a hexagonal plane consisting of several regions of cells. Each cell is labeled with (x, y), where x denotes the hop count from the cell to the MPP, and y denotes its type. Stations in cells of the same type are assumed to leave the cells with the same routing pattern out of certain symmetry. For labeling, every region is partitioned into six congruent segments through diagonal chords such that cells within each segment are labeled in the following manner.

1) From center (0, 0) outward, mark cells along the diagonal line as $(x, 0)$, with an increment of 1 in x. When done, reset x to 2.
2) Initializing y to 1, mark cells with x hops away from the MPP, in an arc-like form, clockwise as (x, y), with an increment of 1 in y.
3) Increase x by 1 and repeat the previous step until no unmarked cells can be found.

Due to such marking in conjunction with Markov chain (see below) reasoning, the simplified random walk model was shown to behave exactly the same as the original 2-D random walks [4]. Consequently, we restrict attention to such a single segment, which is equivalent to considering the extent of a cluster as a whole.

We consider a mesh network of hexagonal cells in that such topology is arguably generic to represent how mesh networking entities are interconnected to cover a geographical area with maximized channel capacities. Concerning handoff in a mesh network, the hop count between a MAP and the MPP forms an essential factor in performing a handoff procedure. While Fig. 9 relates hop counts among cells covered by network entities, cell (0, 0) signifies MPP's radio coverage; other cells are coverages of MAPs connected to this MPP. (We presume that each cell is serviced by a MAP, which also functions as an MP for routing

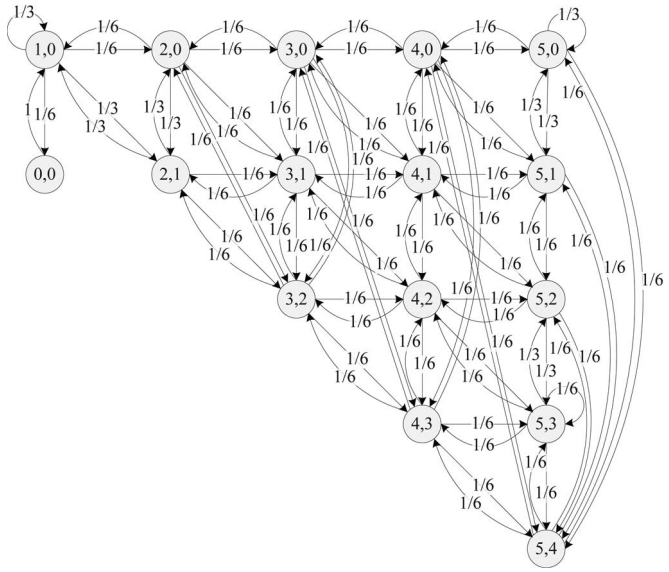

Fig. 10. State transition diagram for a six-subarea cluster.

purposes.) Here, a station residing in a cell is assumed to migrate to any of its neighboring cells with equiprobability of 1/6.

The reduced 2-D random walk model is applicable to capturing a station's movement behavior and obtaining the ratio of inter-MPP handoffs to intra-MPP handoffs occurred in the course. Concerning a random walk process for an n-subarea cluster (e.g., $n = 6$, n indicative of how many levels are present in a cluster), Fig. 10 shows a state transition diagram for a station; state (x, y) indicates a station residing in cell (x, y). Totally, there are $S(n) = (n(n-1)/2) + 1$, $n > 0$ states in an n-subarea cluster. We consider the MPP capable of offering a mobile station a radio link as well; thus, Fig. 10 also depicts the possibility that the station migrates to cell (0, 0).

Let $p_{(x,y),(x',y')}$ be the one-step transition probability from states (x, y) to (x', y') due to handoff. For a six-subarea cluster, the transition probability matrix $\mathbf{P} = [p_{(x,y),(x',y')}]$ is

$$\mathbf{P} = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 1/6 & 1/3 & 1/6 & 1/3 & \cdots & 0 & 0 \\ 0 & 1/6 & 0 & 1/3 & \cdots & 0 & 0 \\ 0 & 1/3 & 1/3 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1/6 & 1/6 \\ 0 & 0 & 0 & 0 & \cdots & 1/6 & 0 \end{bmatrix}_{S(6)\times S(6)}. \tag{1}$$

In $\mathbf{P}$, rows and columns are indexed in order of states $(0,0)$,$(1,0)$,$(2,0)$, $(2,1)$, $\ldots$, $(n-1,0)$, $(n-1,1)$, $(n-1,2)$, $\ldots$, and $(n-1, n-2)$. The general form of $\mathbf{P} = [p_{(x,y),(x',y')}]$ for an n-subarea cluster is given in (6), shown at the bottom of the next page, where

$$w_0\left((x,y),(x',y')\right) = \begin{cases} 1/6, & \text{if } x' = x+1 \text{ and } y' = y \\ 0, & \text{otherwise} \end{cases}$$

$$w_1\left((x,y),(x',y')\right) = \begin{cases} 1/6, & \text{if } x' = x+1 \text{ and} \\ & y' = (y+x'-1) \bmod x' \\ 0, & \text{otherwise} \end{cases}$$

$$w_2\left((x,y),(x',y')\right) = \begin{cases} 1/6, & \text{if } x' = x \text{ and} \\ & y' = (y+x'-1) \bmod x' \\ 0, & \text{otherwise} \end{cases}$$

$$w_3\left((x,y),(x',y')\right) = \begin{cases} 1/6, & \text{if } x' = x-1 \text{ and} \\ & y' = (y+x'-1) \bmod x' \\ 0, & \text{otherwise} \end{cases}$$

$$w_4\left((x,y),(x',y')\right) = \begin{cases} 1/6, & \text{if } x' = x-1 \text{ and} \\ & (y' = x' = 0 \text{ or} \\ & \quad y' = y \bmod x') \\ 0, & \text{otherwise} \end{cases}$$

$$w_5\left((x,y),(x',y')\right) = \begin{cases} 1/6, & \text{if } x' = x \text{ and} \\ & y' = (y+1) \bmod x' \\ 0, & \text{otherwise} \end{cases}$$

$$w_6\left((x,y),(x',y')\right) = \begin{cases} 1/6, & \text{if } x' = x+1 \text{ and} \\ & y' = (y+1) \bmod x' \\ 0, & \text{otherwise} \end{cases}$$

$$v_0\left((x,y),(x',y')\right) = \begin{cases} 1/6, & \text{if } x' = x = n-1 \text{ and} \\ & (y+y') \bmod (n-1) = 0 \\ 0, & \text{otherwise} \end{cases}$$

$$v_1\left((x,y),(x',y')\right) = \begin{cases} 1/6, & \text{if } x' = x = n-1 \text{ and} \\ & (y+y') \bmod (n-1) = 1 \\ 0, & \text{otherwise.} \end{cases}$$

Letting X_i be the random variable representing the mobile station in which state at step i, element $p_{(x,y),(x',y')}$ in $\mathbf{P}$ is given by $\Pr[X_{i+1} = (x', y') | X_i = (x, y)]$, which is the probability of going to (x', y') on the next step, provided that the station currently resides in state (x, y).

Let $\Pi = [\pi_{(0,0)}, \pi_{(1,0)}, \ldots, \pi_{(n-1,n-2)}]$ be the stationary distribution, where $\pi_{(x,y)}$ denotes the equilibrium probability of finding the station in state (x, y). We obtain Π by solving the following two equations:

$$\Pi = \Pi\mathbf{P} \tag{2}$$

$$\pi_{(0,0)} + \sum_{x=1}^{n-1} \sum_{y=0}^{x-1} \pi_{(x,y)} = 1. \tag{3}$$

Since one of the rows in (2) is linearly dependent on the others, it is necessary to introduce the additional conservation relationship as given in (3) to obtain Π. From Π, we can derive the ratio of inter-MPP handoffs to intra-MPP handoffs accordingly (see Section IV-B). This ratio is used to estimate the expected handoff costs of different schemes because, in our architecture, a station only performs four-way handshake during intra-MPP handoff and IEEE 802.1X authentication during inter-MPP handoff. In contrast, IEEE 802.11i requires IEEE 802.1X authentication in each handoff unless the PMK is cached at the target MAP. (PMK can be found in the MAP's cache when preauthentication ahead of handoff has been completed or when the station visited the MAP before, whose corresponding

security context remains in credit.) Such operational differences will lead to distinct performance results.[2]

Note that our Markov chain is constructed in states' points of view. State (x, y) may refer to corresponding cells in different clusters; state (x, y) is interpreted to consolidate all the cells labeled with (x, y) of different clusters in the system. Such unification can be done because of high-symmetry cluster layouts. As such, $\pi_{(x,y)}$ is the aggregate probability of finding the mobile station in cell (x, y) of any cluster. Thus, $p_{(x,y),(x',y')}$ may implicitly subsume intercluster transition probabilities. Taking Fig. 9 as an example, two transitions from border cells (5, 0) to (5, 1) are possible, causing one intercluster and one intracluster handoffs. Thus, $p_{(5,0),(5,1)} = (1/6) + (1/6) = 1/3$. Provided $p_{(x,y),(x',y')}$, the fraction of intercluster transitions is pertinent to the station's whereabouts, as shall be substantiated in Section IV-B.

B. Handoff Latency

We are now in a position to discuss intra-MPP and inter-MPP handoff latencies. As depicted in Fig. 5, the intra-MPP handoff procedure in our architecture involves two messages (for PMK verification) exchanged between the target MAP and the MPP, four-way handshake messages between the station and the MPP, and a message containing a PTK distributed by the MPP to the target MAP. In general, intra-MPP handoff delay L_{INTRA} is composed of authentication latency $L_{\mathrm{INTRA\_AUTH}}$ and four-way handshake latency $L_{\mathrm{INTRA\_4W}}$. These measures can be formulated using several notations.

1) x is the hop count between a MAP and the MPP.
2) S counts MAPs in a concerned segment with x hops to the MPP (see the gray area in Fig. 9). Note that $S = 1$ if $x = 0$; otherwise, $S = x$ for $x \geq 1$.
3) A segment of an n-subarea cluster contains $1 + n(n - 1)/2$ MAPs (including the MPP), as exemplified in Fig. 9.

Therefore, on average, we have

$$L_{\mathrm{INTRA\_AUTH}} = 2 \cdot T \cdot H \tag{4}$$

where T denotes the expected single-hop transmission delay, and H is the mean hop count between a MAP and the MPP, namely

$$H = \frac{\sum_{x=0}^{n-1} (x \cdot S)}{1 + n(n-1)/2}. \tag{5}$$

H results from averaging all possible hop counts over the total number of MAPs within a segment.

In the handshake phase, four-way messages are delivered between the station and the MPP (message exchanges between the station and the intermediary MAP causing a delay of L_{4W}), followed by an additional message for sending a PTK to the target MAP. Hence, we have

$$L_{\mathrm{INTRA\_4W}} = L_{4W} + 5 \cdot T \cdot H. \tag{7}$$

Concerning IEEE 802.11i intra-MPP handoff, IEEE 802.1X authentication is performed if the PMK is not cached at the target MAP. Thus, the average authentication delay $L'_{\mathrm{INTRA\_AUTH}}$ results in

$$L'_{\mathrm{INTRA\_AUTH}} = L_{1X} + M_{\mathrm{RADIUS}} \cdot T \cdot H \tag{8}$$

where L_{1X} is the time required to transport IEEE 802.1X traffic between the station and its Authentication Server, excluding that spent over the mesh backbone. IEEE 802.1X message delay over the mesh backbone is singled out as $M_{\mathrm{RADIUS}} \cdot T \cdot H$, where M_{RADIUS} is the number of RADIUS messages delivered between the target MAP and the MPP. Note that four-way handshake delay in IEEE 802.11i remains as L_{4W}.

Using (8), the mean intra-MPP handoff delay L'_{INTRA} in IEEE 802.11i is[3]

$$L'_{\mathrm{INTRA}} = (1 - P_{\mathrm{PMK\_MISS}}) \cdot L_{4W} + P_{\mathrm{PMK\_MISS}} \cdot (L'_{\mathrm{INTRA\_AUTH}} + L_{4W}). \tag{9}$$

$P_{\mathrm{PMK\_MISS}}$ denotes the probability of a PMK being absent in the target MAP. Given the probability P_v that the station moves to a previously visited authenticator and the probability P_{PF} of IEEE 802.11i preauthentication failure, we find

$$P_{\mathrm{PMK\_MISS}} = (1 - P_v) \cdot P_{\mathrm{PF}}. \tag{10}$$

[2]Another way is to model the station appearing at a random cell, making a number of handoffs (represented with a random variable), and eventually disappearing. The expectation can then be computed over two random variables, i.e., the starting cell and the number of handoffs made in the course.

$$p_{(x,y),(x',y')} = \begin{cases} 6 \times w_0\left((0,0),(x',y')\right), & \text{if } x=y=0 \\ \sum\limits_{i=\{0,1,2,4,5,6\}} w_i\left((x,0),(x',y')\right), & \text{if } 0<x<n-1 \text{ and } y=0 \\ \sum\limits_{i=\{0,2,3,4,5,6\}} w_i\left((x,y),(x',y')\right), & \text{if } 0<x<n-1 \text{ and } 0<y<x \\ \sum\limits_{i=\{2,4,5\}} w_i\left((x,0),(x',y')\right) + 2 \times v_0\left((x,0),(x',y')\right) + v_1\left((x,0),(x',y')\right), & \text{if } x=n-1 \text{ and } y=0 \\ \sum\limits_{i=\{2,3,4,5\}} w_i\left((x,y),(x',y')\right) + v_0\left((x,y),(x',y')\right) + v_1\left((x,y),(x',y')\right), & \text{if } x=n-1 \text{ and } 0<y<x \end{cases} \tag{6}$$

P_{PF} arises when the station moves to a target MAP before its initiated preauthentication is not yet completed. This corresponds to a sudden premature handoff.[3]

Note that the intra-MPP handoff delay in our architecture is L_{INTRA}, which is generally by far lower than L'_{INTRA} incurred in IEEE 802.11i. If a station moves to a new MAP before preauthentication is completed, $L_{\mathrm{INTRA\_AUTH}}$ should still be included in our intra-MPP handoff delay.

Next, consider inter-MPP handoff. L_{INTER} represents the inter-MPP handoff delay for a station in our architecture, equating IEEE 802.1X authentication latency $L_{\mathrm{INTER\_AUTH}}$ and four-way handshake latency $L_{\mathrm{INTER\_4}W}$. With reference to Fig. 6, when the station moves out of a cluster but its valid PMK is not cached at the new target MPP, IEEE 802.1X authentication with a delay of $L_{\mathrm{INTER\_AUTH}}$ remains necessary. To quantify

$$L_{\mathrm{INTER\_AUTH}} = L_{1X} + M_{1X} \cdot (n-1) \cdot T \tag{11}$$

where M_{1X} is the number of IEEE 802.1X messages exchanged between the target MAP and the MPP, and $(n-1)$ is the hop count between the target MAP and the new MPP. Since a station doing inter-MPP handoff will reassociate with some boundary MAP in another cluster, the hop count between the target MAP and the new MPP is thus $(n-1)$. With $L_{\mathrm{INTER\_4}W}$ denoting the average latency for four-way handshake and PTK distribution during inter-MPP handoff, we have

$$L_{\mathrm{INTER\_4}W} = L_{4W} + 5 \cdot (n-1) \cdot T. \tag{12}$$

Inter-MPP handoff in the context of IEEE 802.11i resembles intra-MPP handoff in the form of (8), except that messages are forwarded via the boundary MAP. The incurred authentication latency yields

$$L'_{\mathrm{INTER\_AUTH}} = L_{1X} + M_{\mathrm{RADIUS}} \cdot (n-1) \cdot T. \tag{13}$$

Overall, provided (10) and (13), the inter-MPP handoff delay L'_{INTER} in IEEE 802.11i results in

$$L'_{\mathrm{INTER}} = (1 - P_{\mathrm{PMK\_MISS}}) \cdot L_{4W} + P_{\mathrm{PMK\_MISS}} \cdot (L'_{\mathrm{INTER\_AUTH}} + L_{4W}). \tag{14}$$

From (4), (5), and (14), it can be seen that the handoff delay for a station amounts to

$$L_S = L_{\mathrm{INTER}} \cdot (\Pi \mathbf{Q}) + L_{\mathrm{INTRA}} \cdot (1 - \Pi \mathbf{Q}) \tag{15}$$

where $\mathbf{Q} = [q_{(0,0)}, q_{(1,0)}, q_{(2,0)}, q_{(2,1)}, \ldots, q_{(n-1,n-2)}]^T$ is a column vector of probabilities. Each entry of $\mathbf{Q}$ takes the form $q_{(x,y)}$, which is the probability for the station performing inter-MPP handoff from cell (x, y). The aforementioned equation expresses the mean handoff delay experienced by a station moving in the network. The measure L_S takes the weighted sum of inter-MPP and intra-MPP handoff delays, starting mobility from any cell (x, y). For the former, the weight is the product of $\pi_{(x,y)}$ and the probability $q_{(x,y)}$ of inter-MPP handoff occurrences. Likewise, the weight of intra-MPP handoff delay involves the probability complementary to that for inter-MPP handoffs. Now that a station migrates to any of its neighbor cells with equiprobability, we have $q_{(n-1,0)} = 1/2$ and $q_{(n-1,y)} = 1/2$ for $y = 1, 2, \ldots, n-2$, but otherwise, $q_{(x,y)} = 0$.

Notice that, in our scheme, inter-MPP handoff brings about IEEE 802.1X authentication delay only if a station moves to a new domain before its intended preauthentication can be completed. Thus, the demand for IEEE 802.1X authentication is substantially reduced. In essence, we trade multihop transmissions of four-way handshake messages between a MAP and the MPP within a same administrative domain for expensive cross-realm IEEE 802.1X authentication. Such a design is of value as long as IEEE 802.1X authentication takes a longer delay than that for conveying handshake messages within a regional cluster. As shall be seen shortly in Section IV-D, it is imperative to select the parameter n moderately for scalability considerations.

C. Signaling Traffic

Similar to the foregoing treatment, we now formulate the amount of signaling traffic (number of message transmissions) incurred in intra- and inter-MPP handoff procedures, respectively, over the mesh backbone. Observe that intra-MPP handoff involves authentication traffic $M_{\mathrm{INTRA\_AUTH}}$ and four-way handshake traffic $M_{\mathrm{INTRA\_4}W}$. As illustrated in Fig. 5, our approach requires seven message transmissions over the wireless infrastructure: two messages for PMK verification, four-way handshake messages, and one message for PTK distribution. Hence

$$M_{\mathrm{INTRA\_AUTH}} = 2 \cdot H \tag{16}$$

$$M_{\mathrm{INTRA\_4}W} = 5 \cdot H \cdot R \tag{17}$$

where R is the ratio of four-way handshake to IEEE 802.1X authentication in average message size. Equation (17) reflects a normalized expression for two different sizes of messages in a unified scale. With (16) and (17) and corresponding measures, intra-MPP handoff signaling traffic takes the form

$$M_{\mathrm{INTRA}} = (1 - P_{\mathrm{PMK\_MISS}}) \cdot M_{\mathrm{INTRA\_4}W} + P_{\mathrm{PMK\_MISS}} \cdot (M_{\mathrm{INTRA\_AUTH}} + M_{\mathrm{INTRA\_4}W}). \tag{18}$$

With regard to intra-MPP handoff within IEEE 802.11i, Fig. 2 shows that only RADIUS messages are transmitted. Therefore, $M'_{\mathrm{INTRA\_AUTH}} = M_{\mathrm{RADIUS}} \cdot H$, but $M'_{\mathrm{INTRA\_4}W}$ is zero. The resulting handoff signaling traffic can still be expressed by (18) but with $M'_{\mathrm{INTRA\_AUTH}}$ and

[3]The value of P_{PF} varies from station to station, depending on the following: 1) the elapsed time from the point when such advance operations are initiated to the point when the station disassociates from the current MAP (preauthentication to a target MAP cannot be done if the station loses contact with its current MAP) and 2) the time required to complete preauthentication over the network (network dynamics such as congestion or variable transmission rates govern how long preauthentication message exchanges can take). As opposed to formulating P_{PF} in terms of the two determinants through probabilistic modeling as in [6], this study does not resolve P_{PF} but considers all its possible values ranging between 0 and 1 in Section IV. We then discuss performance results from different settings of P_{PF} to demonstrate general system behavior.

$M'_{\mathrm{INTRA\_4W}}$ in place of $M_{\mathrm{INTRA\_AUTH}}$ and $M_{\mathrm{INTRA\_4W}}$, respectively.

For the inter-MPP handoff case, let M_{INTER} represent the amount of signaling traffic generated due to a station performing inter-MPP handoff, containing authentication traffic $M_{\mathrm{INTER\_AUTH}}$ and four-way handshake traffic $M_{\mathrm{INTER\_4W}}$. In our architecture, as shown in Fig. 6, all EAPOL and four-way handshake messages are transmitted over the mesh infrastructure. Thus, $M_{\mathrm{INTER\_AUTH}} = M_{1X} \cdot (n-1)$ and $M_{\mathrm{INTER\_4W}} = 5 \cdot (n-1) \cdot R$.

As for IEEE 802.11i, inter-MPP handoff causes the same number of message exchanges as in intra-MPP handoff. It follows that $M'_{\mathrm{INTER\_AUTH}} = M_{\mathrm{RADIUS}} \cdot (n-1)$ and $M'_{\mathrm{INTER\_4W}} = 0$. Thus, inter-MPP handoff signaling traffic can be written as

$$M_{\mathrm{INTER}} = (1 - P_{\mathrm{PMK\_MISS}}) \cdot M_{\mathrm{INTER\_4W}} + P_{\mathrm{PMK\_MISS}} \cdot (M_{\mathrm{INTER\_AUTH}} + M_{\mathrm{INTER\_4W}}). \quad (19)$$

The preceding equation also holds for the IEEE 802.11i scheme with $M'_{\mathrm{INTER\_AUTH}}$ and $M'_{\mathrm{INTER\_4W}}$ in lieu of $M_{\mathrm{INTER\_AUTH}}$ and $M_{\mathrm{INTER\_4W}}$, respectively.

In the presence of (18) and (19), the handoff signaling traffic M_S in terms of a cluster gives

$$M_S = M_{\mathrm{INTER}} \cdot (\Pi\mathbf{Q}) + M_{\mathrm{INTRA}} \cdot (1 - \Pi\mathbf{Q}). \quad (20)$$

The measure M_S quantifies the amount of signaling traffic caused by a station doing handoffs in the mesh network. M_S counts all possible transmissions of signaling messages out of inter-MPP and intra-MPP handoffs. The weights of the two types of handoff are identical to those in (15).

D. Performance Results

To validate our analytical model and demonstrate performance results, we developed a simulator in C# that mimicked mobile stations moving about within a clustered environment, as shown in Fig. 9. Under consideration were 100 000 stations, each being simulated to start off from a randomly chosen cell, make 800 cell-crossing movements, and bring in an accumulation of intra-MPP or inter-MPP handoff costs. A station performing an inter-MPP handoff, e.g., to cell (x', y') of another cluster, was taken to emerge next at the corresponding cell (x', y') of the current cluster in that all clusters were considered congruent in appearance. For data representativeness, our simulation results assume the average behavior of all the stations.

Additionally, experiments were conducted to determine parameter values of concern. As shown in Fig. 11, the experimental environment consists of an Authentication Server, two authenticators, and a supplicant station residing in a wireless LAN without any other entities attached. The supplicant station is a laptop PC, which is equipped with an IEEE 802.11g network interface, running on Windows XP SP2 with built-in Windows Zero Configuration Service. Authenticators are another IEEE 802.11g-capable PCs running the open-source daemon hostapd-0.5.7. The Authentication Server employs FreeRADIUS-1.1.4. All these four machines are kept synchronized to the same Network Time Protocol server throughout. The encryption protocol in use is WPA2/AES, and the EAP method is PEAP/EAP-MSCHAPv2. A widely used packet analyzer—Wireshark—is run on the supplicant station and the Authentication Server sides to capture all the packets of interest.

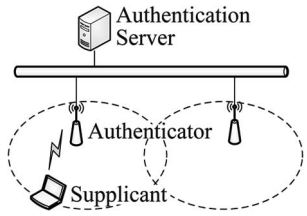

Fig. 11. Experimental environment.

TABLE I
SYSTEM PARAMETERS

T	2.44 ms
L_{1X}	401.63 ms
L_{4W}	20.76 ms
M_{1X}	22 messages
M_{RADIUS}	18 messages
R	1.0492

TABLE II
MEAN P_v

$n = 1$	0.000000
$n = 2$	0.064579
$n = 3$	0.120625
$n = 4$	0.164704
$n = 5$	0.199851
$n = 6$	0.229387
$n = 7$	0.254347
$n = 8$	0.275391

Table I summarizes the average values of system parameters resulting from 20 full authentication processes, where T is, in particular, out of 80 measurements. In addition, we built n-subarea clusters and carried out 1 200 000 independent identical simulations of random walks to resolve the ratio P_v that a cell-crossing station migrates to a previously visited authenticator. The collected statistics of P_v in different n-subarea settings are listed in Table II. Note that a network environment where authenticators are colocated at MAPs corresponds to the setting $n = 1$, which is a typical IEEE 802.11s scenario.

According to IEEE 802.11s [13], the suggested level of a mesh network is 3 (i.e., $n = 3$). Hence, we elaborate primarily on the performance in terms of a three-subarea clustered environment. Fig. 12(a) plots handoff delay L_S versus P_{PF} in an n-subarea network environment. Overall, our numerical results conform closely with simulation results. In addition, this figure reveals a trend that our proposal reduces handoff delays significantly. In particular, when P_{PF} is 1.0, i.e., the station does not perform preauthentication,[4] our approach can achieve a saving of handoff delay by up to 268%, which is a marked improvement. Therefore, our design is of utility, although most IEEE 802.11 devices do not support preauthentication. As a

[4]The preauthentication function in Windows XP with WPA2 is disabled by default.

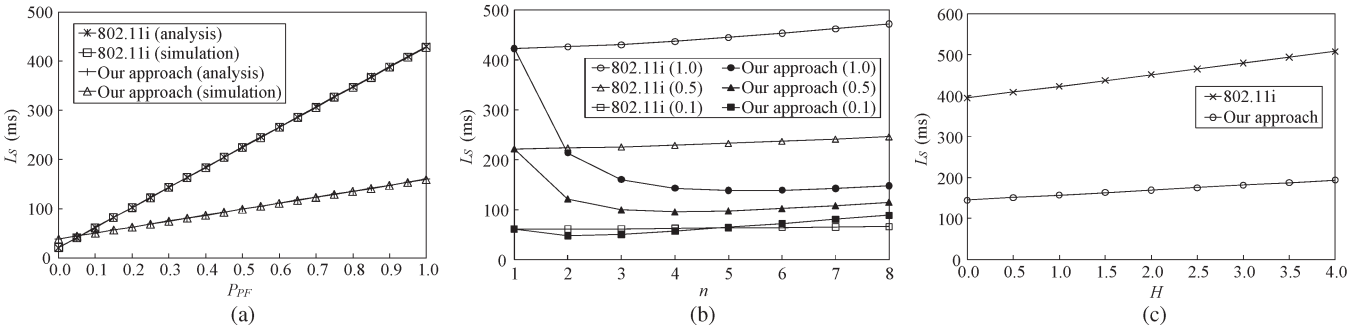

Fig. 12. Handoff delays of two subject schemes. (a) L_S versus $P_{\rm PF}$ $(n = 3)$. (b) L_S versus n. (c) L_S versus H $(n = 3;\ P_{\rm PF} = 1.0)$.

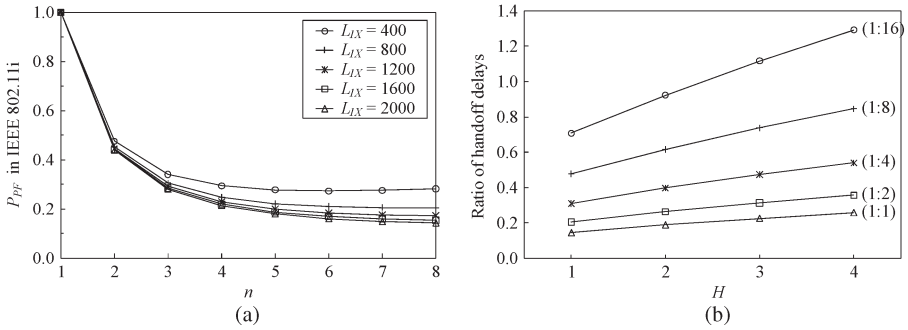

Fig. 13. Handoff delay of our approach relative to the counterpart scheme. (a) $P_{\rm PF}$ versus n. (b) Handoff delay comparison versus H.

note, our approach maintains its advantage over the counterpart scheme unless $P_{\rm PF} < 0.05$, which, however, signifies a rare case. This case arises because four-way handshake messages forwarded between a MAP and the MPP bring about comparatively longer delay in our architecture.

Further experiments in other settings reflect a consistent trend that numerical results accord with simulation results substantially, which justifies the correctness of our analytical model. For conciseness and clarity reasons, hereinafter, we provide analytical results as main parts of figure layouts.

Fig. 12(b) shows handoff delays under different cluster sizes and preauthentication failure probabilities ($P_{\rm PF}$ is represented in parenthetical numbers of the legends). This figure suggests that, as long as the cluster is large enough, e.g., with $n \geq 3$, handoff delays appear immaterially different for whichever $P_{\rm PF}$, meaning that $P_{\rm PF}$ becomes a less dominant factor for a sufficiently large network. Hence, for a concise presentation, we next confine ourselves to discussing performance results from $P_{\rm PF}$ that is equal to 1.0. Performance statistics in other $P_{\rm PF}$ settings can be proportionately estimated with reference to Fig. 12(a).

From Fig. 12(b), it can be seen that, when n is 5, our approach results in the least handoff delay. Indeed, the handoff delay in our architecture appears indistinct if $n \geq 3$. This finding is justifiable, since as n grows larger, a mobile station is more likely to experience intra-MPP handoff upon a move (saving costly IEEE 802.1X authentication), but meanwhile, it suffers more hop-by-hop transmissions of four-way handshake messages between a MAP and the MPP. In other words, the increasing overhead of multihop transmissions for four-way handshake messages may counteract the benefit brought by a larger cluster when n becomes sufficiently large. For IEEE 802.11i, a similar argument applies. That is, the larger n grows, the more multihop transmissions (longer delay) of EAP traffic are required. Thus, L_S increases with n.

With regard to the effect of different network topologies, Fig. 12(c) shows handoff delays relating to the changes of mean hop count H between a MAP and the MPP. Fig. 12(c) results from experiments by varying the parameter S in (5). Varying S implies a floating number of MAPs with certain hops away from the MPP, thereby leading to different interconnectivity of MAPs. Performance results show that our approach can reduce the handoff delay of the counterpart scheme by an appreciable amount, resulting in a reduction of around 63%.

Let us investigate under what conditions the two subject schemes exhibit comparable handoff delay. To gain fairer bases for comparison, we vary L_{1X} in a large extent, representing possible scenarios. Here, suppose that our approach operates with $P_{\rm PF}$ preset to 1.0. Supposing that both schemes are made to produce nearly identical handoff delay, we are now concerned with the relationship between $P_{\rm PF}$ in the IEEE 802.11i scheme and the cluster parameter n. Fig. 13(a) indicates that our proposed approach achieves almost equivalent effectiveness resulting from the IEEE 802.11i scheme, with $P_{\rm PF}$ ranging between 0.15 and 0.3. This means that, effectively, our approach functions as if the IEEE 802.11i scheme were operating with high likelihood of 70%–85% successful preauthentication, without resorting to additional facilities such as handoff prediction techniques, network topology information, or profiles of handoff behavior.

Observe that system-wide performance is also subject to which entities enact the role of the IEEE 802.1X authenticator and how frequent reauthentication processes or PTK updates take place. When a MAP acts as an authenticator, the system involves heavier outlays for PMK distribution and reauthentication but less overhead for four-way handshake

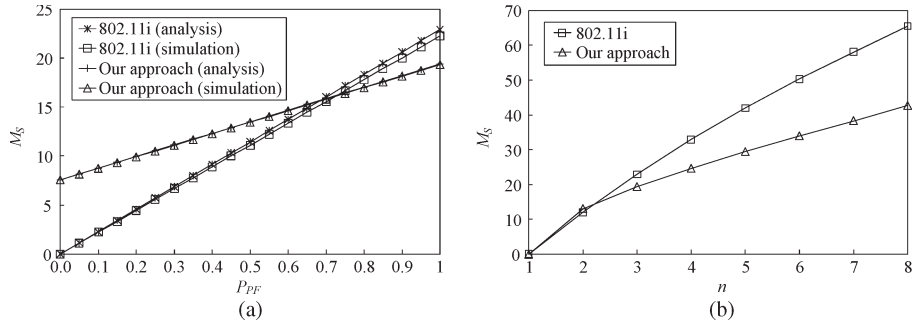

Fig. 14. Signaling traffic of two subject schemes. (a) M_S versus $P_{\rm PF}$ ($n = 3$). (b) M_S versus n ($P_{\rm PF} = 1.0$).

due to PTK updates. On the other hand, an MPP behaving as an authenticator contributes to fewer messages for PMK distribution and reauthentication but at the expense of more signaling overhead for renewing PTKs in that four-way handshake always goes to the MPP. Similar arguments for handoff delay apply here as well. Since IEEE 802.1X (re)authentication (PMK updates) and PTK updates occur at times, their resulting effects are of interest. Fig. 13 compares their incurred delays in different cases of PMK or PTK updates carried out at varying frequencies with different hop count H. It can be seen that our approach remains advantageous unless PTK updates appear comparatively too often. However, as evidenced in [14], a PTK is arguably allocated with lifetime on the order of several hours. Therefore, it is deduced that PTK updates are mostly occasional and less likely to cause overwhelming counteraction.

Handoff signaling traffic is another performance aspect. In this regard, Fig. 14(a) shows the relationship between M_S and $P_{\rm PF}$ when $n = 3$. Again, this figure exhibits osculating results from analytical and simulation models without apparent discrepancies. However, this figure shows that our approach may lose its advantage over the IEEE 802.11i scheme in certain circumstances. To be more specific, when $P_{\rm PF} < 0.7$, our approach generates more signaling traffic than the IEEE 802.11i scheme does. This is mainly because our proposed approach assumes a centralized architecture, where any generated four-way handshake messages are conveyed to some MPP over multihop mesh links, causing more transmissions than those induced by IEEE 802.1X authentication. Nevertheless, Fig. 14(a) depicts that signaling traffic is kept low in a few tens, placing an insignificant burden on the network.

Fig. 14(b) shows M_S under different cluster sizes for $P_{\rm PF} = 1.0$. Results indicate that the overall handoff signaling traffic generated by our approach is less than that by the IEEE 802.11i scheme, except for $n = 2$. (For $n = 2$, our signaling traffic is slightly higher.) This reflects the cost effectiveness of our approach in that the benefit due to restricting most signaling traffic within a larger cluster outvalues the potential overhead of increased multihop transmissions.

Further extensive evaluation reveals that signaling traffic in both schemes grows linearly with average hop count H between a MAP and the MPP. Given $n = 3$, $P_{\rm PF} = 1.0$, and H ranging over the interval [0, 4], for instance, we find that the IEEE 802.11i scheme generates signaling traffic in quantity of 8.33–54.98, whereas our approach generates signaling traffic in quantity of 12.94–33.59. Our approach is found to introduce less handoff signaling traffic than the counterpart scheme does throughout our experiments. This implies that our design caters better to a variety of network topologies.

Cross referencing Figs. 12–14 gives a more thorough view of how and when the proposed approach outperforms the conventional scheme. These figures delimit the usefulness of our approach in practical sense, assuring that our approach is suited where a mesh network is neither too small nor unduly large in scale. (An excessively large network is liable to suffer overwhelming overhead of message exchanges.) The foregoing discussions corroborate that a network of MAPs or MAPs with a maximum of three hops to the MPP adopting our approach operates fairly well, even in the absence of any preauthentication support.

To summarize, performance results indicate that our approach is promising if MPs or MAPs are organized into MPP-centric clusters, each with approximately 19–37 MPs that are interconnected to an MPP. Such cluster size of several tens in order is agreeable to the suggested scale of a mesh network by IEEE 802.11s [13]. As another remark, our approach allows MPs to be clustered in moderate size such as to minimize IEEE 802.1X authentication while keeping inter-MP communication within the cluster manageable. This facilitates a battery-powered mobile station to balance its power consumption and handoff performance. Note that our scheme comes to some limitation in scalability (overloading the MPP) when cluster size grows unduly large. Nevertheless, Figs. 12–14 lead us to argue that the proposed scheme suffices for real mesh networks.

V. Conclusion

This paper has presented an approach to secure fast handoff in an IEEE 802.11s mesh network, which is a field that warrants closer study. Our approach reduces repeated IEEE 802.1X authentication processes and encryption/decryption processing of data frames for mobile stations by an appreciable amount. Our development exhibits several features. First, the security level in line with IEEE 802.11i is maintained. Section III-D has reasoned that our approach does not lead to security vulnerability. Nor did we trade performance for security and robustness to the extent that security requirements for IEEE 802.11i or 802.11s are unduly weakened. Furthermore, our scheme prevents PMKs from being distributed over the wireless medium, protecting against any unauthorized access from the air.

Second, following our design tenet, the entities holding pairwise master keys are shifted to MPPs in a way that fast handoff can be accomplished by bypassing prohibitive IEEE

802.1X authentication during handoff. Such a design enables the setup of an end-to-end secure communication channel—a bidirectional MAC tunnel—between a station and its MPP to keep data frame exchanges intact in the mesh environment.

Meanwhile, our approach is characterized by backward and forward compatibility; we leverage the use of standard protocols at the station side without tailoring a current protocol fabric. Hence, interoperability with IEEE 802.11i- or 802.11s-conformant devices is maintained. In addition, our approach may serve as an optional, but not a costly, add-on to any IEEE 802.11-based mesh network. Note that original security and routing mechanisms predefined in IEEE 802.11s can fully cooperate with our development.

Moreover, Section IV provided an analytical model to formulate handoff delay and incurred signaling overhead. With our analysis in place, an optimal number of MAPs managed by an MPP (or the best location of an IEEE 802.1X authenticator somewhere between a MAP and the MPP) can be determined accordingly. Performance results have demonstrated the strengths of our proposed approach and augur well for our design in practical application.

To conclude this paper, we outline several future directions to work on. First, we continue implementing our approach using hostapd, which is a widespread open-source platform. Second, it is apropos to relate our analytical model to evaluating handoff methodology in other contexts, e.g., IEEE 802.11r or 802.16e (Worldwide Interoperability for Microwave Access). Derived analytical results can give an indication of how these handoff processes perform in a quantitative fashion, which may become part of feasible studies on any subsequent development. Third, we note that reauthentication mechanisms of EAP methods shall undergo some optimization for seamless handoff in mobile wireless environments. There has been active work in progress in a new Internet Engineering Task Force workgroup, which is called *Handover Keying*. We are keeping closely aligned with the development of the new workgroup. Finally, our treatment can be extended to other types of multihop wireless networks by allowing network entities within the same domain (analogous to MPs in the mesh architecture) to share out the workload of four-way handshake and encryption and decryption in frame delivery. While such an extension entails context transfers among network entities, APs that are accommodating mobile stations need to keep up with adjustments of new authenticators. This suggests a topic that warrants more thorough investigation in the future.

ACKNOWLEDGMENT

The authors would like to thank G. K.-L. Huang for helpful discussions and the anonymous reviewers for valuable comments on earlier drafts of this paper.

REFERENCES

[1] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)," IETF Network Working Group, RFC 3748, Jun. 2004.

[2] B. Aboba, D. Simon, and P. Eronen, Extensible Authentication Protocol (EAP) Key Management Framework, IETF Network Working Group, Internet Draft ⟨draft-ietf-eap- keying-22.txt⟩, Nov. 2007.

[3] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: A survey," *Comput. Netw.*, vol. 47, no. 4, pp. 445–487, Mar. 2005.

[4] I. F. Akyildiz, Y.-B. Lin, W.-R. Lai, and R.-J. Chen, "A new random walk model for PCS networks," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 7, pp. 1254–1260, Jul. 2000.

[5] A. Alimian and B. Aboba, Analysis of Roaming Techniques, IEEE 802.11 Contribution 802.11-04/0377r1, Mar. 2004.

[6] K.-H. Chi, C.-C. Tseng, and Y.-H. Tsai, "Fast handoff among IEEE 802.11r mobility domains," *J. Inf. Sci. Eng.*, vol. 26, no. 4, pp. 1345–1362, Jul. 2010.

[7] K.-H. Chi, J.-H. Jiang, and L.-H. Yen, "Cost-effective caching for mobility support in IEEE 802.1X frameworks," *IEEE Trans. Mobile Comput.*, vol. 5, no. 11, pp. 1547–1560, Nov. 2006.

[8] W. S. Conner, J. Kruys, and J. C. Zuniga, IEEE 802.11s Tutorial: Overview of the Amendment for Wireless Local Area Mesh Networking, Dallas, TX, IEEE 802 Plenary, Nov. 2006.

[9] H. Duong, A. Dadej, and S. Gordon, "Proactive context transfer and forced handover in IEEE 802.11 wireless LAN based access networks," *ACM Mobile Comput. Commun. Rev.*, vol. 9, no. 3, pp. 32–44, Jul. 2005.

[10] *Port-Based Network Access Control*, IEEE Std. 802.1X-2004, Dec. 2004.

[11] *Amendment 6: Medium Access Control (MAC) Security Enhancements*, IEEE Std. 802.11i-2004, Jul. 2004.

[12] *Amendment 2: Fast BSS Transition*, IEEE Std. P802.11r, Jul. 2008.

[13] *Amendment: ESS Mesh Networking*, IEEE Std. Draft P802.11s/D2.0, Apr. 2008.

[14] P. Kiratiwintakorn and P. Krishnamurthy, "An energy efficient security protocol for IEEE 802.11 WLANs," *Pervasive Mobile Comput.*, vol. 2, no. 2, pp. 204–231, Apr. 2006.

[15] M. Lasserre and V. Kompella, IETF Network Working Group, Virtual private LAN service (VPLS) using label distribution protocol (LDP) signaling, RFC 4762, Jan. 2007.

[16] A. Mishra, M. H. Shin, and W. Arbaugh, "An empirical analysis of the IEEE 802.11 MAC layer handoff process," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 33, no. 2, pp. 93–102, Apr. 2003.

[17] A. Mishra, M. H. Shin, and W. Arbaugh, "Context caching using neighbor graphs for fast handoffs in a wireless network," in *Proc. 23rd IEEE INFOCOM*, 2004, pp. 351–361.

[18] A. Mishra, M. H. Shin, N. L. Petroni, Jr., T. C. Clancy, and W. A. Arbaugh, "Proactive key distribution using neighbor graphs," *IEEE Wireless Commun.*, vol. 11, no. 1, pp. 26–36, Feb. 2004.

[19] S. Pack and Y. Choi, "Fast inter-AP handoff using predictive authentication scheme in a public wireless LAN," in *Proc. IEEE Netw. Conf.*, Aug. 2002, pp. 15–26.

[20] S. Pack and Y. Choi, "Pre-authenticated fast handoff in a public wireless LAN based on IEEE 802.1x model," in *Proc. IFIP Pers. Wireless Commun. Conf.*, Oct. 2002, pp. 175–182.

[21] S. Pack, J. Choi, T. Kwon, and Y. Choi, "Fast handoff support in IEEE 802.11 wireless networks," *Commun. Surveys Tuts.*, vol. 9, no. 1, pp. 2–12, Mar. 2007.

[22] 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 Comput. Commun. Rev.*, vol. 9, no. 4, pp. 39–49, Oct. 2005.

[23] M. G. Rahman and H. Imai, "Security in wireless communication," *Wireless Pers. Commun.*, vol. 22, no. 2, pp. 213–228, Aug. 2002.

[24] M. H. Shin, A. Mishra, and W. Arbaugh, "Improving the latency of 802.11 hand-offs using neighbor graphs," in *Proc. 2nd Int. Conf. Mobile Syst., Appl., Services*, 2004, pp. 70–83.

[25] G. Xue, "An improved random walk model for PCS networks," *IEEE Trans. Commun.*, vol. 50, no. 8, pp. 1224–1226, Aug. 2002.

Kuang-Hui Chi (M'04) received the B.S. degree in computer science and engineering from Tatung University, Taipei, Taiwan, in 1991 and the M.S. and Ph.D. degrees in computer science and information engineering from National Chiao Tung University, Hsinchu, Taiwan, in 1993 and 2001, respectively.

He is currently an Associate Professor with the Department of Electrical Engineering, National Yunlin University of Science and Technology, Touliu, Taiwan. His current research interests include wireless Internet and protocol verification.

Dr. Chi is a member of the Association for Computing Machinery.

Yung-Chien Shih is currently working toward the Ph.D. degree in computer science and information engineering with National Chiao Tung University, Hsinchu, Taiwan.

He is currently with Telcordia Applied Research Center Taiwan Company, Taipei, Taiwan. His current research interests include wireless mesh networks and telematics.

Ho-Han Liu received the M.S. degree in computer science and information engineering from National Chiao Tung University, Hsinchu, Taiwan, in 2007.

He is currently a senior engineer with Taiwan Semiconductor Manufacturing Company, where he designs and operates large-scale wireless Local Area Networks.

Jui-Tang Wang received the Ph.D. degree in computer science and information engineering from National Chiao Tung University, Hsinchu, Taiwan, in 2008.

He is currently with the Information and Communications Research Laboratories, Industrial Technology Research Institute, Hsinchu. His current research interests include Worldwide Interoperability for Microwave Access networks and Long-Term Evolution technologies.

Shiao-Li (Charles) Tsao (M'04) received the Ph.D. degree in engineering science from National Cheng Kung University, Tainan, Taiwan, in 1999.

From 1999 to 2003, he was with the Computers and Communications Research Laboratories, Industrial Technology Research Institute (ITRI), as a Researcher and a Section Manager. He is currently an Associate Professor with the Department of Computer Science, National Chiao Tung University, Hsinchu, Taiwan. He was a Visiting Professor with the University of Waterloo, Waterloo, ON, Canada, in the summer of 2007 and with the Swiss Federal Institute of Technology Zurich, Zurich, Switzerland, in the summer of 2010. He has published more than 70 international journal and conference papers. He is the holder of 18 U.S. patents. His research interests include mobile communication and wireless networks and embedded software and systems.

Prof. Tsao was a recipient of the Research Achievement Award from ITRI in 2000 and 2004, the Highly Cited Patent Award from ITRI in 2007, the Outstanding Project Award from the Ministry of Economic Affairs (MOEA) in 2003, and the Advanced Technologies Award from MOEA in 2003. He was also a recipient of the Young Researcher Award from the Pan Wen-Yuan Foundation, the Young Engineer Award from the Chinese Institute of Electrical Engineering in 2007, the Outstanding Teaching Award from the National Chiao Tung University, and the K. T. Li Outstanding Young Scholar Award from the Association for Computing Machinery Taipei/Taiwan chapter in 2008.

Chien-Chao Tseng received the B.S. degree in industrial engineering from National Tsing Hua University, Hsinchu, Taiwan, in 1981 and the M.S. and Ph.D. degrees in computer science from the Southern Methodist University, Dallas, TX, in 1986 and 1989, respectively.

He is currently a Professor with the Department of Computer Science, National Chiao Tung University, Hsinchu. His research interests include wireless Internet, handover techniques for heterogeneous networks, and mobile computing.