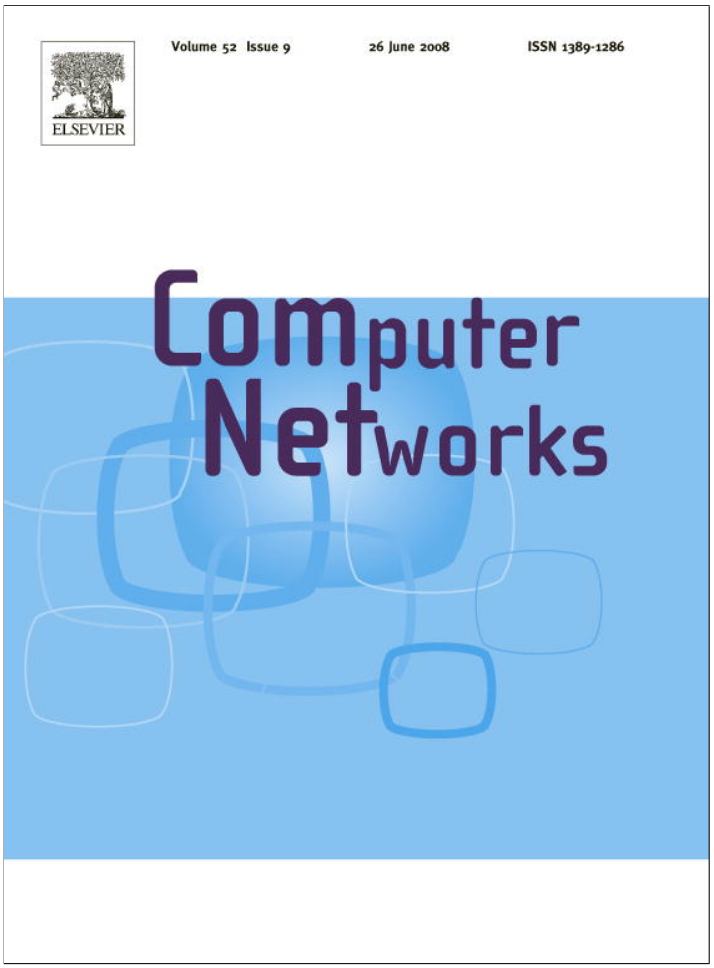

Computer Networks 52 (2008) 1693–1702

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

# User authentication and undeniable billing support for agent-based roaming service in WLAN/cellular integrated mobile networks

Minghui Shi [a], Xuemin (Sherman) Shen [a,*], Jon W. Mark [a], Dongmei Zhao [b], Yixin Jiang [a]

[a] Electrical and Computer Engineering Department, University of Waterloo, 200 University Avenue W., Waterloo, Ontario, Canada N2L 3G1
[b] Electrical and Computer Engineering Department, McMaster University, Hamilton, Ontario, Canada

ARTICLE INFO

*Article history:*
Received 17 December 2007
Accepted 18 February 2008
Available online 13 March 2008

Responsible Editor: L.G. Xue

*Keywords:*
Authentication
Billing
Agent
Roaming service
WLAN/cellular integrated network

ABSTRACT

In this paper, a framework of authentication and undeniable billing support for an agent-based roaming service in WLAN/cellular networks interworking networks is proposed. This framework circumvents the requirement of peer-to-peer roaming agreements to provide seamless roaming service between WLAN hotspots and cellular networks operated by independent wireless network service providers. Within the framework, an adaptive authentication and an event-tracking scheme have been developed, which allow the application of undeniable billing service to cellular network even when it still uses a traditional authentication scheme. The proposed modified dual directional hash chain (MDDHC) based billing support mechanism features mutual non-repudiation. Security analysis and overhead evaluation demonstrate that the proposed framework is secure and efficient.



## 1. Introduction

Wireless local area network (WLAN) functionality has become the de facto standard component in mobile devices. More and more WLAN hotspots serviced by wireless internet service providers (WISPs) have been deployed in airports, cafes, book stores, etc. Mobile devices having both cellular phone and WLAN capability are available [1]. The mobile users naturally demand integrating multiple mobile computing services into a single entity.

Fig. 1 illustrates the interworking between WLAN and 3G cellular networks through an IP network. Mobile IP (MIP) protocol [2,3] is applied to support IP mobility for mobile clients. Data can be transported along two different paths, as shown in dashed lines in the figure, depending on which access interface that the mobile terminal is associated with. The home agent (HA) and the foreign agent (FA) are added to support mobile IP. The gateway GPRS serving node (GGSN) is modified to act as a FA for the cellular network. The WLAN hotspot may have its gateway as a FA. The mobile terminals (MTs) are provided with MIP clients and can support both IEEE 802.11 and 3G access technologies. Depending on the inter-dependence between WLAN and the cellular network, the coupling between them can be tight or loose. In tight-coupling, the IEEE 802.11 network injects data directly to the 3G core network and therefore appears to the 3G core network as another 3G access network via WLAN packet data gateway (PDG). Tight-coupling is usually preferred by the cellular network carriers for their own WLAN hotspots. In loose-coupling, the IEEE 802.11 gateway connects to the Internet and does not have any direct link to 3G network elements. Depending on the ownership of the WLAN hotspots, a loosely coupled integrated architecture is preferred [4] due to its flexibility by independent hotspots, and a tightly coupled architecture is used by cellular network carrier owned hotspots.

* Corresponding author. Tel.: +1 519 888 4567x32691; fax: +1 519 746 3077.
*E-mail addresses:* mshi@bbcr.uwaterloo.ca (M. Shi), xshen@bbcr.uwaterloo.ca (Xuemin (Sherman) Shen), jwmark@bbcr.uwaterloo.ca (J.W. Mark), dzhao@mail.ece.mcmaster.ca (D. Zhao), yixin@bbcr.uwaterloo.ca (Y. Jiang).

1389-1286/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2008.02.012

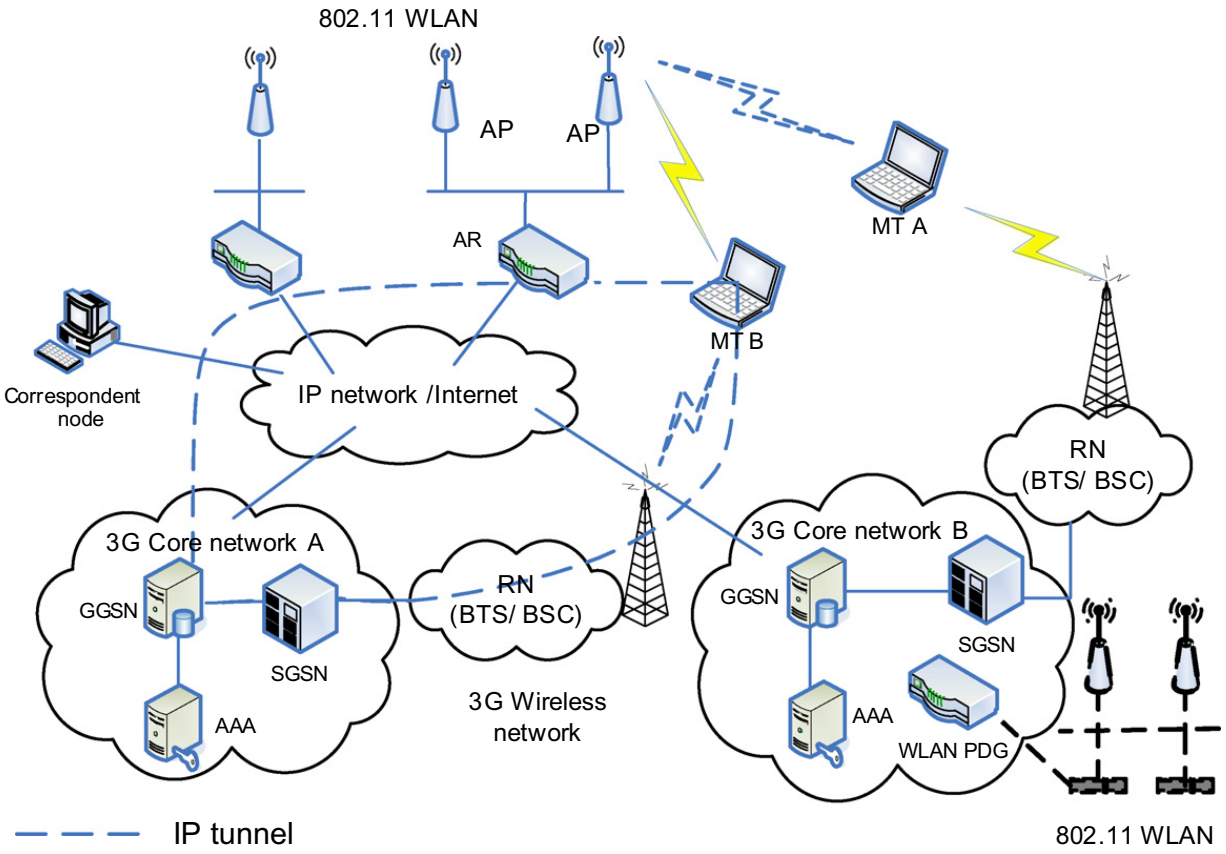


**Fig. 1.** Integrated 802.11 WLAN and 3G cellular networks.

Although user roaming is well defined in cellular network through authentication, authorization and accounting (AAA), it is still an open issue in WLAN networks operated by multiple service providers. Many WISPs provide public WLAN Internet access at the hotspots using network access server (NAS), which lacks inter-domain roaming and mobile IP support. We expect much more WLAN hotspots to be deployed by much more WISPs service providers than the cellular counterpart, because of the simplicity and low cost of setting up a WLAN hotspot. However, it is difficult for a service provider to have a roaming agreement with all other network service providers. Therefore, in such a case, the traditional peer-to-peer roaming agreement mechanism is impractical, or at least inefficient, especially for independent WLAN hotspot service providers, and universal roaming service cannot be achieved. Billing support across network carriers could be an issue considering there is no direct roaming agreement. When the service provider is metering the network usage by the MT, it may have problem in determining whether the MT has left the service session if it is shut down abnormally due to power, software and/or network glitches.

Most of the WLAN/cellular network interworking research work focuses on proposing integration architecture [5] and modifying network components, such as gateway [6], analyzing switching performance of integrated service [7]. However, most solutions are suitable for the service providers who operate their own WLAN and cellular networks. In [8], a roaming and authentication architecture for WLAN/cellular network integration is proposed. However, the billing support, which has become important properties for roaming services, is not considered. In [9], a single hash chain based undeniable billing support is proposed, where digital signature is applied to the MT side to prevent the FA from falsely claiming extended service to the MT. Due to the heavy computation of digital signature, it may not be desirable due to the fact that MT is a low powered device.

In this paper, an authentication process, integrated with undeniable billing support, for an agent-based wireless/cellular interworked network is proposed. The integrated wireless network service can be offered by independent WLANs and cellular networks, which are not affiliated with peer-to-peer roaming agreements, under the coordination of a service agent (SA). Therefore, many small WLAN service providers are able to join the interworked networks, which could greatly increase the integrated network service coverage. The proposed authentication scheme for integrated network service can be elastically applied to both WLAN and cellular networks, or WLAN alone. Event-tracking for undeniable billing support schemes are parallel to the authentication process, such that they can be flexibly deployed by a network, such as a cellular network, which does not adopt the proposed authentication scheme. Based on a modified dual directional hash chain (MDDHC), the proposed schemes offer mutually undeniable billing support and, at the same time, resource consuming digital signature is avoided. It is shown that the MDDHC based

**Table 1**
Description of symbols

| Symbol | Explanation |
|---|---|
| $ID_X$ | $X$'s identity or a unique global device number |
| $k_i$ | $i$th session key |
| $k_{XY}$ | Shared key between $X$ and $Y$ |
| $Pub_X$ | $X$'s public key |
| $E_k\{\}$ | Symmetric encryption using shared key $k$ |
| $E_k\langle\rangle$ | Asymmetric encryption using public key $k$ |
| $Sig_X$ | Digital signature signed by $X$ |
| $\|\|$ | Concatenation operation |
| $t_s$ | Time stamp |
| $sn_i$ | Serial number |

billing mechanism requires less computation and communication overhead than the method in [9], which makes it more suitable for low power wireless communication devices.

The rest of the paper is organized as follows. In Section 2, an overview of the proposed roaming service framework for cellular/WLAN interworking, including the messaging scheme and event-tracking mechanism for the proposed service model, is presented. Security analysis and overhead evaluation are given in Section 3, followed by concluding remarks in Section 4. The common symbols that will appear in message exchanges thereafter and their explanation are listed in Table 1.

## 2. Agent-based WLAN/cellular integrated service framework

The actual network parties in a roaming scenario have the relationship as shown in Fig. 2. The FA resides in the network that the MT is visiting, which can be either a WLAN or a cellular network. The HA resides in the MT's home network, which knows all information about the MT, such as identification, shared secret key, etc. The SA is introduced, as an additional component, to deal with the roaming agreement issue in the WLAN/cellular interworking network architecture when the number of WLAN operators is large, and therefore service flexibility is improved. Cellular networks and WLANs are encouraged to have centralized roaming agreement with the SA directly so that cumbersome peer-to-peer roaming agreements are no longer needed. A service provider optionally sets up peer-to-peer agreement with a few major service providers for better performance, and also sets up a centralized roaming agreement with the SA for completion of universal roaming.

As shown in Fig. 2, the proposed roaming service framework is composed of two layers: authentication/registration plane and event-tracking plane for billing support. Considering the well developed authentication scheme in a cellular network, the proposed authentication can be used by WLAN alone for smooth and economic integrated service deployment. Meanwhile, the event-tracking, which is a key component for integrated service billing function, can be uniformly adopted by all network operators with little modifications, especially in a cellular network. A new business model in the integrated service offering by the proposed roaming service framework is that the SA can also provide cellular/WLAN integrated service by itself. The SA contracts bulk wireless service from physical network operators and sells wireless integrated service to the customers so that network operators pay less support cost for end users. The proposed framework also enables customers to receive improved network access convenience and the SA to get more revenue.

### 2.1. Service session setup

#### 2.1.1. Overview of dual directional hash chain

We first introduce the concept of one-way hash function, which is the foundation of the DDHC. A hash function Hash(.) takes a binary string of arbitrary length as input, and outputs a binary string of fixed length. A one-way function $H$ satisfies the following two properties: (1) given $x$, it is easy to compute $y$ such that $y = \text{Hash}(x)$; and (2) given $y$, it is computationally infeasible to compute $x$ such that $y = \text{Hash}(x)$. The security features of the proposed group-wise key distribution schemes are based on one-way property of hash function.

A one-way hash chain, as illustrated by forward or backward hash chains in Fig. 3, is formed by recursively hashing $x$ and lining them up in sequence. Let us take the forward hash chain as an example. Due to the one-way

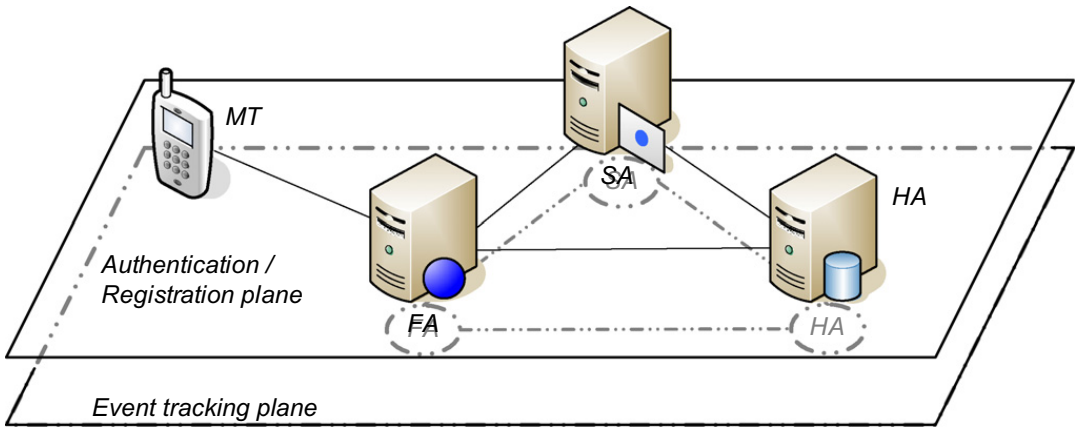


**Fig. 2.** Service model function and messaging scheme overview.

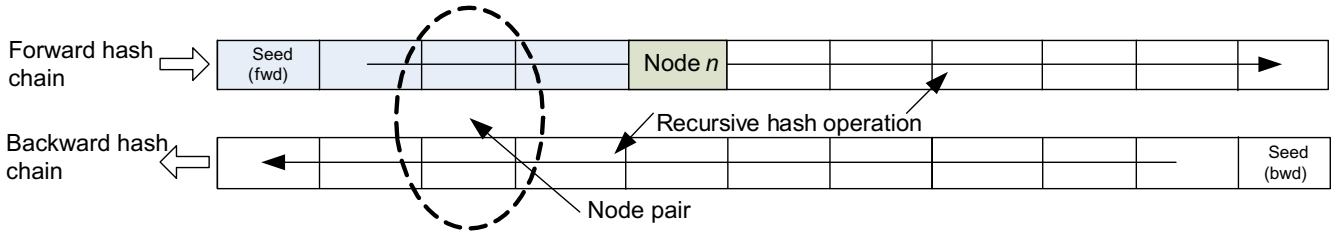


**Fig. 3.** Structure of dual directional hash chain. Note that the arrows along the forward and backward hash chains indicate the direction of hash operations to generate the node series.

property of the hash function, given any value of node $n$ in the chain, it is computationally infeasible to calculate the forward elements, but is easy to compute backward elements.

A DDHC (Fig. 3) is composed of two one-way hash chains with equal length: a forward hash chain and a backward hash chain. It can be derived as follows: (1) Generating two random key seed values, seed (fwd) and seed (bwd), for the forward and the backward hash chains, respectively; (2) repeatedly applying the same one-way function on each seed to generate two hash chains of equal length.

The DDHC offers both forward and backward secrecy. Given the end nodes of a window within the chain, the combination of the corresponding nodes in the forward and backward chains offers security measure in terms of that a party cannot generate the node pairs outside the window.

### 2.1.2. Dual directional hash chain setup at MT

In the proposed framework, the DDHC is modified to suite the particular use for billing support in mobile communications environment. MDDHC is used to refer DDHC in this paper thereafter. As shown in Fig. 4, the MT sets $H(k_{\mathrm{MH}}||rnd_n)$ as the seed for backward chain, where $k_{\mathrm{MH}}$ is the shared secret key between the MT and the HA, and $rnd_n$ is the random number of $n$th MDDHC. The MT sets $H(k_{\mathrm{MH}}||\overline{rnd_n})$ as the seed for forward chain, where $\overline{rnd_n} = NOT(rnd_n)$.

The mask window begins from the time when the service session is started, and ends at the time when the service session is terminated. The concept of node pair only applies to the beginning end of the window. In this particular DDHC application, the forward hash chain ends at the node of "service started" since it is no longer needed for protecting service session beyond that point.

Assume $t_{\mathrm{billing}}$ is the metering unit of billing. During its idle time, the MT generates multiple MDDHCs with length $l_n = \lceil T/t_{\mathrm{billing}} \rceil$, and different *rnd*s, where $T$ should be a bit longer than typical maximum service session duration. The MT only stores the nodes of the entire backward hash chain, the seed of the forward hash chain, and the corresponding *rnd*.

## 2.2. Authentication and service request scheme

Before the MT accesses the network service, authentication is performed to verify the legitimacy of both the MT and service provider, and the MT is registered in the network if it is authenticated successfully. In the authentication plane shown in Fig. 2, the SA acts as an authority, which is trusted by all the parties, and assists mutual validation of the FA and the HA. By considering the low capability of the MT and wireless transmission environment, the authentication scheme is designed such that most of the authentication process is executed by servers in the wired network.

### 2.2.1. Adaptive user authentication process

We briefly introduce the normal mode of the authentication process for the proposed service agent-based WLAN/cellular integrated roaming service framework followed by the description of the inherited sub-sets for variations. Assume an MT is accessing a WLAN hotspot (FA) for the first time. Fig. 5 shows the message flow of the proposed authentication scheme. The major authentication stages in the figure are described as follows.

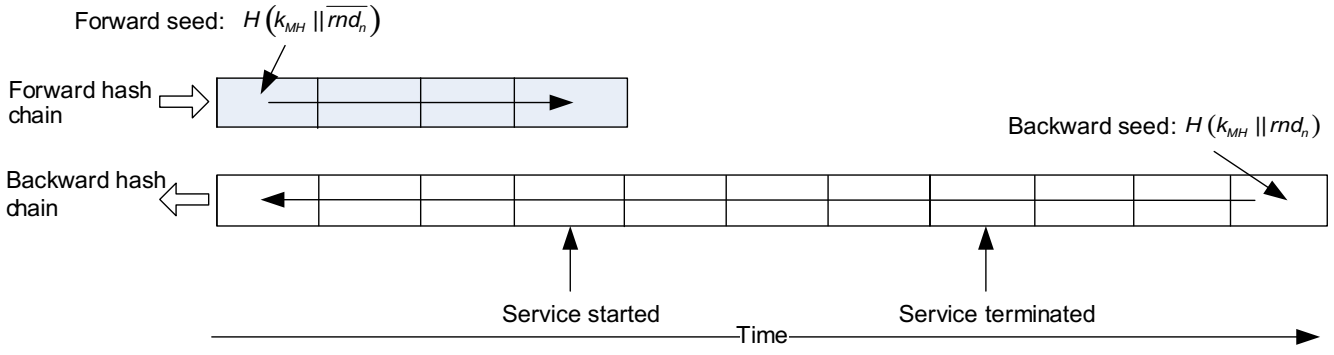


**Fig. 4.** MDDHC setup at MT.

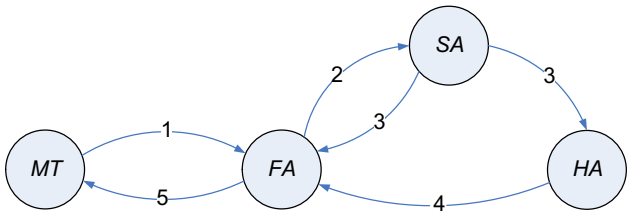


**Fig. 5.** General authentication message flow of the proposed authentication scheme.

1. The MT submits the authentication request and the wrapped session key to be negotiated to the FA. The MT can use its International Mobile Subscriber Identity (IMSI) for $ID_M$, and sends Message (1) to the FA with current time stamp $ts_1$

$$M \rightarrow F : ID_M||ID_H||E_{k_{MH}}\{ID_M||N_M||k_i||ts_1\}, \quad (1)$$

   where $ID_M||ID_H$ represents modified AAA user name in the form of username@domain.
2. The FA forwards the Message (1) to the SA and requests the HA for verification. The FA sets $Msg_M = ID_M||ID_H||E_{k_{MH}}\{ID_M||N_M||k_i||ts_1\}$, and sends Message (2) to the SA

$$F \rightarrow S : ID_F||E_{k_{SF}}\{Msg_M||sn_i||ts_2\} : sig_F. \quad (2)$$

3. The SA returns identity information of the HA, and forwards the authentication message from the MT to the HA. The SA sets $Msg_F$ to $Msg_M||sn_i||ts_2$ and sends Message (3) to the HA:

$$S \rightarrow H : ID_S||ID_F||pub_F||E_{k_{SH}}\{Msg_F||ts_3\} : sig_S, \quad (3)$$

   and sends Message (4) to the FA:

$$S \rightarrow F : ID_S||ID_H||pub_H||ts_3 : sig_S. \quad (4)$$

4. The HA verifies the identities of the MT by matching the $ID_M \leftrightarrow k_{MH}$ mapping in its user database, and returns the session key to the FA. The HA sends Message (5) to the FA:

$$H \rightarrow F : ID_H||E_{k_F} < N_M||k_i||ID_M||ts_4 >: sig_H. \quad (5)$$

5. The FA gets $ID_S$, the nonce $N_M$ and the session key $k_i$ proposed by the MT in (1), which shows the HA has acknowledged the existence of the MT and approved its roaming privilege. The FA generates a ticket $Tk_i = TkID_i||ref_i||exp_i$, where $TkID_i$ denotes the ticket ID, $ref_i$ denotes the ticket reference code, and $exp_i$ denotes the ticket expiration time. The FA stores the mapping relationship $Tk_i \leftrightarrow k_i \leftrightarrow ID_M$. The FA sends the proof of the knowledge of the session key (6) to the MT:

$$F \rightarrow M : ID_F||E_{k_i}\{H(N_M)||N_F||Tk_i||ts_5\}. \quad (6)$$

   The MT chooses a node pair at or close to the left end of an available $MDDHC_n$, and sends Message (7) as the acknowledgement of Message and begins to send communication data to the network operated by the FA

$$M \rightarrow F : ID_S||E_{k_i}\{H(N_F)||rnd_n||l_n||x_n||y_{x_n}||ts_6||comm\_data\}, \quad (7)$$

where $rnd_n$, $l_n$ and $x_n$ denotes the random component of the seed, length of $MDDHC_n$ and the position of the start endpoint of the window of $MDDHC_n$, and $y_{x_n}$ denotes the node pair at $x_n$ of the $MDDHC_n$. Then the MT and the FA have been mutually authenticated. $k_i$ can be used to encrypt the communication between the MT and the FA.

After receiving Message (7) from the MT, the FA retrieves and stores $rnd_n$, $l_n$, $x_n$ and $y_{x_n}$ as part of the metering record of the on-going service session. The recorded parameters are used to form Event ID, which will be introduced in Section 2.3.

The proposed authentication scheme self-adapts to various service scenarios. When the MT re-visits the FA, or the MT visits any hotspot operated by the FA for the second time or more, FA and MT can authenticate each other using cached ticket ID. A subset of the proposed authentication scheme, which is composed of Step 1, Step 5 and Step 6, is executed, as follows:

$$M \rightarrow F : ID_M||TkID_i||E_{k_i}\{ref_i||N_M||k_{i+1}||ts_1\}, \quad (8)$$
$$F \rightarrow M : ID_F||E_{k_{i+1}}\{H(N_M)||N_F||Tk_{i+1}||ts_5\}, \quad (9)$$
$$M \rightarrow F : ID_M||E_{k_{i+1}}\{H(N_F)||rnd_n||l_n||x_n||y_{x_n}||ts_6||comm\_data\}. \quad (10)$$

Note that in this case, the FA assumes that the MT's account at the HA is in a healthy status. The HA should notify the FA to revoke the ticket once it finds out that the MT is no longer good. The most recent FA list that served the MT can be obtained by searching the Event IDs in the MT's service record. If the MT re-visits the FA after $exp_i$ timeout, a full authentication process is required as described in the above subsection. In addition, based on Steps 1, 5 and 6, the following two scenarios are also supported: (1) The MT accesses a network (WLAN hotspot, for example) operated by its home network when it is in the home network; (2) the MT accesses WLAN hotspots operated by the visiting cellular network, which supports ticket and PID.

The proposed scheme supports a new business model in which the integrated service is offered by the SA. In such a case, it is a win–win situation for all three parties: the MT has more flexibility of wireless network access, the SA gains higher revenue, and the network carriers receive less support calls from end users. In such "integrated service offered by the SA" scenario, the MT does not belong to any real network operator and it only registers with the SA, which is denoted as SA′ for notational convenience. Therefore, SA′ is considered as the MT's home network and takes over the work which is designated to the HA in Section 2.2.1. Since the FA and the SA have direct service agreement and share a pre-set secret key, the public key exchange in Step 3 is not necessary, and thus asymmetric encryptions are avoided. The subset of the proposed authentication scheme, which is composed of all the steps except Step 3 with minor parameter modifications, is executed as follows:

$$M \rightarrow F : ID_M||ID_S||E_{k_{MS}}\{ID_M||N_M||k_i||ts_1\}; \quad (11)$$
$$F \rightarrow S : ID_F||E_{k_{SF}}\{Msg_M||sn_i||ts_2\} : sig_F; \quad (12)$$
$$S \rightarrow F : ID_S||E_{k_{SF}}\{N_M||k_i||ID_M||ts_4\} : sig_S; \quad (13)$$
$$F \rightarrow M : ID_F||E_{k_i}\{H(N_M)||N_F||Tk_i||ts_5\}; \quad (14)$$
$$M \rightarrow F : ID_M||E_{k_i}\{H(N_F)||rnd_n||l_n||x_n||y_{x_n}||ts_6||comm\_data\}. \quad (15)$$

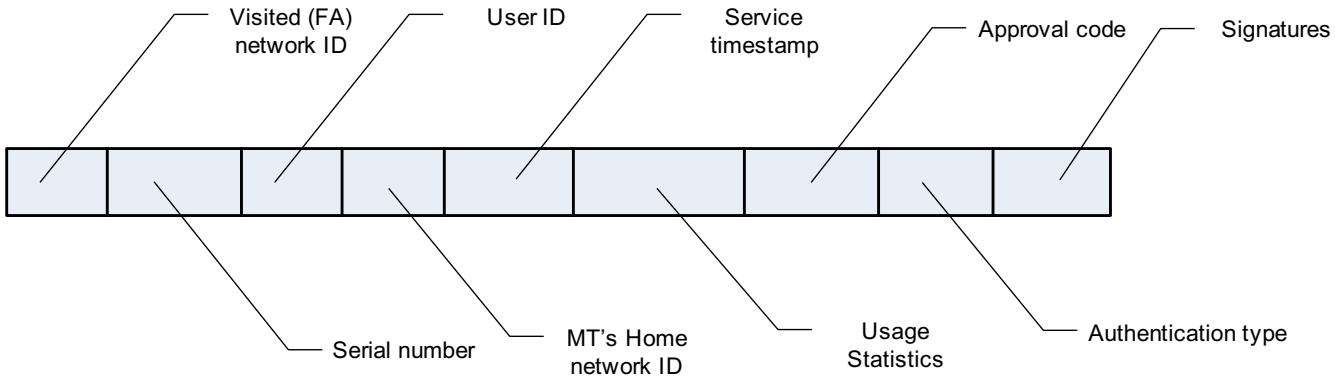


**Fig. 6.** Event ID date structure.

When peer-to-peer roaming agreement exists between the HA and the FA, the only change is to replace SA by HA in the above messages. Note that the HA and the FA have shared secret key $k_{HF}$ in this case.

### 2.3. Event-tracking for billing support

Commercial network service deployment cannot be released without a billing mechanism. In the proposed WLAN/cellular integrated service model, billing is based on the MT's network accessing activities. We assume that the WLAN/cellular integrated service is offered by multiple regional networks under different administration. The mobile user will get single bill periodically, such as monthly, from its home network. The charge by the foreign networks for the service to the mobile user will also go through the home network. The billing charge is based on the time of usage, which is measured by the length of MDDHC. Note that the proposed billing support can also be applied to network traffic based charge, in which case the length of MDDHC represents the network traffic instead of service time, as shown in this work.

#### 2.3.1. Heart beat of MT

When the MT is accessing the service offered by the FA, starting from $y_{x_n+1}$, the MT periodically releases nodes one by one, or heart beat, along the time in the backward hash chain of the MDDHC at around metering interval:

$$M \rightarrow F : \mathrm{ID}_M || E_{k_i}\{y_{x_{n+j}} || \mathrm{ts}\}, \tag{16}$$

where $j$ denotes the metering interval passed. Upon receiving Message (16), the FA updates service end value by overwriting $y_{x_{n+j-1}}$ by $y_{x_{n+j}}$. When the MT finishes the service session at node $J$ normally, the FA should have the node pair $y_{x_n}$ as service session start value and the node $y_{x_{n+J}}$ as service session end value. If the service session is terminated abnormally, the FA will not receive the heart beat any more. After pre-determined grace period, the FA uses the latest $y_{x_{n+j}}$ as the final service session end value. If the FA receives the heart beat within the grace period, the FA continues the service session and updates the service session end value using the received $y_{x_{n+j}}$. The effect of missing a few heart beats to proper billing can be neglected. Such measure solves incorrect billing when the MT does not disconnect from the service session based on normal procedure.

Sometimes the service session may be longer than the length of one MDDHC. In such a case, the MT should be aware of this case since it knows the total length of the MDDHC-in-use. The MT will do a ticket ID type authentication with the FA to apply another MDDHC in background. Such situation is viewed by the network as two consecutive service sessions from any aspect. Since the FA has the information of total length of the MDDHC-in-use, it can predict the upcoming authentication, such as fetch the MT's ticket credential into the cache, etc.

#### 2.3.2. Distribution of Event ID

The activity of the MT is tracked by a data structure named Event ID as shown in Fig. 6. An event is defined as an incident of the MT accessing the network resource. An Event ID is distributed to proper network operators by the event-tracking process, which is running independently from the authentication process. The revenue is partitioned later based on the Event ID records.

Most data fields in Fig. 6 have either appeared in previous literature or are self-explanatory. The usage statistics field includes the MT network activities data, such as connection time, upload/download traffic bandwidth, zone and/or service weight, etc. How to adopt these parameters into billing generation solely depends on the roaming agreements and is beyond the scope of this work. Approval code is a reference number indicating that the event claim is approved by the MT's home network. The attested signatures from involved network operators show that they agreed with those data.

Based on the nature of billing mechanism, we classify network operators into three categories: (roaming) service provider, home network and (roaming) service coordinator. Table 2 summaries the distribution status of event ID among these roles in the four scenarios. For example, in the "Re-visit" case, the SA is not involved and it is unnecessary to send Event ID to the SA. However, the HA still requires Event ID for billing purpose. "Integrated service offered by SA" is a novel business model which decouples the mobile users and the network operators so that there

**Table 2**
Event ID distribution

| Scenario | Auth. type | Service provider | MT's home network | Service coordinator | Event ID distribution |
|---|---|---|---|---|---|
| Normal | 1 | FA | HA | SA | FA, HA, SA |
| Re-visit | 2 | FA | HA | – | FA, HA |
| Service offered by SA | 3 | FA | SA | – | FA, SA |
| Peer-to-peer roaming agreement | 4 | FA | HA | – | FA, HA |

is no need to treat all network access activities differentially and there is no traditional HA role in this scenario. During authentication process, the network operators keep the received messages at least until Event ID distribution completes. Event-tracking is implemented as follows.

After the FA receives Message (7). the service session starts. Meanwhile, the FA fills in fields of the event ID data structure and constructs

$$\text{Event ID}_i^{\text{FA}} = \text{ID}_F||sn_i||\text{ID}_M||\text{ID}_H||\text{ts}_6||(n||rnd_n||x_n||y_{x_n})||\text{null}||1 : \text{sig}_F, \tag{17}$$

where null indicates not applicable. The FA sends Message (18) to the MT's home agent, which is the HA or, in service type 3, the SA[1]

$$F \to H : \text{ID}_F||E_{k_H}\langle\text{Event ID}_i^{\text{FA}}\rangle. \tag{18}$$

After the HA or the SA receives Message (18), it can re-construct the MDDHC that the MT uses for the corresponding service session by using $rnd_n$ in the Event ID and $k_{\text{MH}}$ that the HA already possesses. Then the HA checks if $y_{x_n}$ matches the node pair at position $x_n$ of the re-constructed MDDHC, i.e., $y_{x_n} = (H^{x_n}(k_{\text{MH}}||\overline{rnd_n}), H^{l_n - x_n}(k_{\text{MH}}||rnd_n))$. If it holds, the HA returns Message (19) to the FA and the SA, respectively

$$\begin{aligned} &H \to S : \text{ID}_H||E_{k_{\text{SH}}}\{\text{Event ID}_i^{\text{FA}}||\text{apv} : \text{sig}_H\}, \\ &H \to F : \text{ID}_H||E_{k_F}\langle\text{Event ID}_i^{\text{FA}}||\text{apv} : \text{sig}_H\rangle, \end{aligned} \tag{19}$$

where apv denotes the approval code. Note that in case of service type 2, 3 and 4, the HA only needs to send Message (19) to the FA.

After the MT finishes the network access session in the service area, such as the hotspots or cellular cells operated by the FA, the FA fills in fields of the event ID data structure and constructs Event $\text{ID}_i^{\text{FA}}$:

$$\text{Event ID}_i^{\text{FA}} = \begin{cases} \text{ID}_F||sn_i||\text{ID}_M||\text{ID}_H||\text{ts}||(n||y_{x_{n+J}})||1 : \text{sig}_F, \\ \quad \text{if Auth. type} = 1 \\ \text{ID}_F||Tk_i||\text{ID}_M||\text{ID}_H||\text{ts}||(n||y_{x_{n+J}})||2 : \text{sig}_F, \\ \quad \text{if Auth. type} = 2 \\ \text{ID}_F||sn_i||\text{ID}_M||\text{ID}_S||\text{ts}||(n||y_{x_{n+J}})||3 : \text{sig}_F, \\ \quad \text{if Auth. type} = 3 \\ \text{ID}_F||sn_i||\text{ID}_M||\text{ID}_H||\text{ts}||(n||y_{x_{n+J}})||4 : \text{sig}_F, \\ \quad \text{if Auth. type} = 4, \end{cases} \tag{20}$$

where ts denotes the latest timestamp since the last Message (16). Similar to the action that FA distributes the Event ID to the HA and/or the SA described earlier, the FA sends the encrypted Event $\text{ID}_i^{\text{FA}}$ in Eq. (20) to the HA or, if the MT's integrated service is offered by the SA. The HA[1] locates the re-constructed $\text{MDDHC}_n$, matches $y_{x_{n+J}}$ along the $\text{MDDHC}_n$ and tries to compute $J$ by the position differentiation of $y_{x_n}$ and $y_{x_{n+J}}$. If the matching process succeeds, i.e., $y_{x_n} = H^{l_n - x_{n+J}}(k_{\text{MH}}||rnd_n)$ is located, the total time of the service is computed as $t_{\text{ss}} = J \cdot t_{\text{billing}}$.

If the service session spans over multiple MDDHC, multiple Event IDs are generated along with the additional ticket ID authentication sessions. The total service session time is $\sum t_{\text{ss},i}$, where $i$ is the corresponding Event ID. Optionally, the HA can check if the MT's is located within the network service provider's physical location by verifying the MT's care-of-address or by location-aware application [10]. If the tests are all passed, the HA or the SA attaches the approval code and its digital signature, and sends Message (21) or (22) to the FA, correspondingly

$$H \to F : \text{ID}_H||E_{k_{\text{FH}}}\{\text{Event ID}_i^{\text{FA}}||\text{apv} : \text{sig}_H\}, \tag{21}$$

$$S \to F : \text{ID}_S||E_{k_{\text{SF}}}\{\text{Event ID}_i^{\text{FA}}||\text{apv} : \text{sig}_S\}. \tag{22}$$

Note that authentication type 2 differs from others. The HA is not notified when the FA offers service to the MT. However, the FA still sends Event ID to the HA. The HA should always notify the FAs where the ticket is still valid for the MT to revoke the ticket if the MT is not in good standing, such as failing to pay the bill by the deadline, etc. Such FAs can be found by searching the Event IDs generated when the MT accesses those FAs for the first time.

## 3. Security and performance analysis

### 3.1. Robustness of the proposed authentication scheme

The proposed security schemes are robust to resist certain attacks and sniffing. The intruder cannot impersonate all parties. In both authentication and event-tracking schemes, the messages between wired parties, such as service providers and service agents, are identified by their digital signatures. The proposed authentication scheme can resist replay and man-in-the-middle attack. The intruder cannot act as the MT since he cannot generate a meaningful Message (1), which can be detected by the HA.

We focus on authentication acceleration when describing the proposed authentication scheme. User anonymity and intractability are important security property, which can be achieved by adopting similar user identity replacement proposed in [11] at the signalling level in the pro-

[1] For simplicity, we use the HA to include both cases.

posed authentication by jointly using other privacy hiding techniques at the internet protocol (IP) and medium access control (MAC) levels.

Replay attack is prevented by implementing an encrypted timestamp mechanism and refreshed nonce. The intruder cannot update the encrypted timestamp in the replayed message, which can be identified by the legitimate users if its timestamp is out of the pre-defined range.

### 3.2. Dispute resolution

The proposed MDDHC based billing support mechanism can avoid repudiation from the FA and the MT. The dispute in this work includes the following cases:

- for the FA, over-claim and false claim the service provided;
- for the MT and the HA, denial of the entire or partial service received[2];
- for the SA, false claim of non-existed service coordination.

The FA may claim more service time offered to the MT. The FA is able to generate the elements on the left hand side of $y_{x_n}$ in the backward hash chain. However, the FA cannot compute the corresponding elements in the forward hash chain due to the one-way property of the hash chain. Similarly, the FA cannot compute the elements on the right hand side of $y_{x_{n+J}}$. Therefore, the knowledge of the MHHDC of FA is limited to the window defined by $y_{x_n} y_{x_{n+J}}$, and it cannot over-claim the actual service session duration time.

The MDDHC's seed is the concatenation of the shared secret key between the MT and the HA, and a random number. While the random number offers the diversity of the MDDHCs, the shared secret key component ensures that the MDDHC at the FA is generated by the MT only. Therefore neither the FA nor the SA is able to generate a valid MHHDC by themselves to falsely claim the service session that does not exist. For the same reason, if the FA holds $y_{x_n}$ and $y_{x_{n+J}}$, it indicates that the MT must have received the entire service during the corresponding time that begins at $x_n$ and ends at $x_n + J$. At the same time, the FA does not need to hold all the elements in between to prove the service usage by the MT. Missing receiving a few $y_{x_{n+j}}$ due to network connectivity problem, etc. is also tolerable to the proposed billing mechanism.

### 3.3. Overhead evaluation and feature comparison

The overhead is crucial since the security protocols are implemented on the mobile devices in the wireless communications environment. Heavy computation by the mobile is not feasible [12]. The bandwidth is lower and the channel error is higher in wireless networks than those in the wired networks, therefore it is also important for the security protocols to minimize the message size and the number of message exchanges.

**Table 3**
Parameters used in overhead analysis

| Parameter | Data length (HEX digits) |
|---|---|
| $ID_M$/PID | 15 |
| ID network (IP address) | 8 |
| Nonce | 16 |
| Session key | 32 |
| Timestamp | 8 |
| Hash function output | 16 |
| Ticket ID | 8 |
| Ref | 4 |
| Exp | 8 |
| Node in MDDHC | 32 |

By applying the dual one-way property of MDDHC, digital signature operation for the billing support, which is costly in both computing and communication, at the MT is not required. Assume that the data length of parameters in authentication messages related to the MT is set as shown in Table 3. The total authentication message exchange via the wireless link is less than 1 kB. The cryptographic algorithm and parameter length can be adjusted to balance communication/computation overhead and security strength.

The cryptographic operations at the MT are symmetric encryption/decryption and hash, which are efficient in computation, communication and power consumption. In order to further reduce the service access latency, the MT pre-computes multiple MDDHCs with different lengths during its idle time so that the MDDHC is immediately available when the MT accesses the service. The storage requirement of the MDDHCs is not high. According to Table 3, if the MT would like to generate one MDDHC for 8 h with metering cycle 2 min, the required storage allocation is 8 kB. In practice, the MT should generate multiple shorter MDDHCs for couples of hours' use, which consumes even less simultaneous storage space.

### 3.4. Characteristics comparison of billing support

The proposed event ID billing support can accommodate various user authentication scenarios in both local and roaming network access. Table 4 shows that the advantages of the proposed billing support scheme over billing support used in cellular network is the capability of adaptively handling special modes, such as re-visiting and agent-based network access service, for the integrated network. Since PID is used to index the usage record, user anonymity is preserved in billing messages.

## 4. Conclusion

A framework of an adaptive authentication process which is integrated with mutual undeniable billing support has been proposed for integrated WLAN/cellular networks. The framework considers the road path of the integration, and can seamlessly adapt to agent-based

[2] We consider the MT and the HA as one group, and the service offered by the FA is received by the MT–HA group because of the security and business relationship between the MT and the HA.

**Table 4**
Comparison of billing support schemes

| | Event ID billing support | Cellular network billing support | Billing support in [9] |
|---|---|---|---|
| Local service | Yes | Yes | Yes |
| Peer-to-peer. roaming auth. | Yes | Yes | Yes |
| Agent-based roaming auth. | Yes | No | No |
| Localized/cached auth. | Yes | No | No |
| Service offered by agent | Yes | No | No |
| Adaptive | Good | Poor | Poor |
| Mutual undeniable | Yes | No | Yes |
| Computation | Low | Low | High |

roaming service, current traditional authentication scenario and future business model. The MDDHC based billing and Event ID tracking mechanism support all wireless integrated service type and provide mutual repudiation protection. It has been shown that the proposed authentication and billing support framework is secure and light weight, and suitable for various roaming scenarios to achieve reduced support cost, more communication convenience and higher revenue.

## Acknowledgement

This work has been partially supported by a Natural Sciences and Engineering Research Council (NSERC) of Canada Postdoctoral Fellowship.

## References

[1] Cisco Systems Inc., Wireless LAN Technologies, Products, & Trends, Technical report, April 2004.
[2] C. Perkins, IP Mobility Support for IPv4, IETF RFC 3344, 2002.
[3] D. Johnson, C. Perkins, J. Arkko, Mobility Support in IPv6, IETF RFC 3775, 2004.
[4] M. Buddhikot, G. Chandranmenon, S. Han, Y.W. Lee, S. Miller, L. Salgarelli, Integration of 802.11 third-generation wireless data networks, Proceedings of IEEE INFOCOM'03 1 (April) (2003) 503–512.
[5] W. Song, W. Zhuang, A. Saleh, Interworking of 3G cellular networks and wireless LANs, International Journal of Wireless and Mobile Computing 2 (2007) 237–247.
[6] V.W.-S. Feng, L.-Y. Wu, Y.-B. Lin, W.E. Chen, WGSN: WLAN-based GPRS environment support node with push mechanism, The Computer Journal 47 (2004) 405–417.
[7] M. Shi, L. Xu, X. Shen, J.W. Mark, A. Saleh, Air interface switching and performance analysis for fast vertical handoff in cellular network and WLAN interworking, Wireless Communications and Mobile Computing (Wiley) 7 (2007) 581–594.
[8] M. Shi, X. Shen, J.W. Mark, IEEE802.11 roaming authentication in wireless LAN/cellular mobile networks, IEEE Wireless Communications 11 (August) (2004) 66–75.
[9] J. Zhou, K.-Y. Lam, Undeniable billing in mobile communications, MOBICOM'98 (1998) 284–290.
[10] M. Hazas, J. Scott, J. Krumm, Location-aware computing comes of age, IEEE Computer 37 (February) (2004) 95–97.
[11] Y. Jiang, C. Lin, X. Shen, M. Shi, Mutual authentication and key exchange protocols for roaming services in wireless mobile networks, IEEE Transactions on Wireless Communication 5 (2006) 2569–2577.
[12] D.S. Wong, A.H. Chan, Mutual authentication and key exchange for low power wireless communications, Proceedings of IEEE Military Communications Conference, MILCOM 2001 1 (2001) 39–43.

**Minghui Shi** received a B.S. degree (1996) from Shanghai Jiao Tong University, China, and an MASc. degree (2002) and a Ph.D. degree (2006) from the University of Waterloo, Ontario, Canada, all in electrical and computer engineering. He is currently with McMaster University, Ontario, Canada as an NSERC (Natural Sciences and Engineering Research Council of Canada) Postdoctoral Fellow and a research associate with the Centre for Wireless Communications, University of Waterloo. His current research interests include wireless LAN/cellular network integration, vehicular communications networks and relevant network security issues.

**Xuemin (Sherman) Shen** received the B.Sc. (1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. He is a Professor and University Research Chair, and the Associate Chair for Graduate Studies, Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research focuses on mobility and resource management in interconnected wireless/wired networks, UWB wireless communications systems, wireless security, and ad hoc and sensor networks. He is a co-author of three books, and has published more than 300 papers and book chapters in wireless communications and networks, control and filtering. Dr. Shen serves as the Technical Program Committee Chair for IEEE Globecom'07, General Co-Chair for Chinacom'07 and QShine'06, the Founding Chair for IEEE Communications Society Technical Committee on P2P Communications and Networking. He also serves as a Founding Area Editor for IEEE Transactions on Wireless Communications; Editor-in-Chief for Peer-to-Peer Networking and Application; Associate Editor for IEEE Transactions on Vehicular Technology; KICS/IEEE Journal of Communications and Networks, Computer Networks; ACM/Wireless Networks; and Wireless Communications and Mobile Computing (Wiley), etc. He has also served as Guest Editor for IEEE JSAC, IEEE Wireless Communications, and IEEE Communications Magazine. Dr. Shen received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004 from the University of Waterloo, the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada, and the Distinguished Performance Award in 2002 from the Faculty of Engineering, University of Waterloo. Dr. Shen is a registered Professional Engineer of Ontario, Canada.

**Jon W. Mark** received the Ph.D. degree in electrical engineering from McMaster University, Canada in 1970. Upon graduation, he joined the Department of Electrical Engineering (now Electrical and Computer Engineering) at the University of Waterloo, became a full Professor in 1978, and served as Department Chairman from July 1984 to June 1990. In 1996, he established the Centre for Wireless Communications (CWC) at the University of Waterloo and has since been serving as the founding Director. He was on sabbatical leave at the IBM Thomas Watson Research Center, Yorktown Heights, NY, as a Visiting Research Scientist (1976–77); at AT&T Bell Laboratories, Murray Hill, NJ, as a Resident Consultant (1982–83); at the Laboratoire MASI, Universit'e Pierre et Marie Curie, Paris, France, as an Invited Professor (1990–91); and at the Department of Electrical Engineering, National University of Singapore, as a Visiting Professor (1994–95). His current research interests are in wireless communications and wireless/wireline interworking, particularly in the areas of resource management, mobility management, and end-to-end information delivery with QoS provisioning.

He is a co-author of the textbook Wireless Communications and Networking (Prentice-Hall, 2003). Dr. Mark is a Life Fellow of the IEEE and has served as a member of a number of editorial boards, including IEEE Transactions on Communications, ACM/Baltzer Wireless Networks, Telecommunication Systems, etc. He was a member of the Inter-Society Steering Committee of the IEEE/ACM Transactions on Networking from 1992–2003, and a member of the IEEE COMSOC Awards Committee during the period 1995–1998.

**Dongmei Zhao** received the Ph.D. degree in Electrical and Computer Engineering from the University of Waterloo, Waterloo, Ontario, Canada in June 2002. Since July 2002 she has been with the Department of Electrical and Computer Engineering, McMaster University, Hamilton, Ontario, Canada where she is an assistant professor. Dr. Zhao's research interests include modeling and performance analysis, quality-of-service provisioning, access control and admission control in wireless cellular networks and local area networks. Dr. Zhao is a member of the IEEE.

**Yixin Jiang** received a Ph.D. degree (2006) from Tsinghua University, China and an ME degree (2002) from Huazhong University of Science and Technology both in Computer Science. In 2005, he is currently a Postdoctoral fellow with Department of Electrical and Computer Engineering, University of Waterloo, Canada. His current research interests include security and performance evaluation in wireless communication and mobile computing.