PPAB: A Privacy-Preserving Authentication and Billing Architecture for Metropolitan Area Sharing Networks

Haojin Zhu, Xiaodong Lin, Minghui Shi, Pin-Han Ho, *Member, IEEE*, and Xuemin (Sherman) Shen, *Fellow, IEEE*

***Abstract*—Wireless metropolitan area sharing networks (WMSNs) are wide-area wireless networks with nodes owned and managed by independent wireless Internet service providers (WISPs). To support seamless roaming in emerging WMSNs, in this paper, we propose a localized and distributed authentication and billing architecture that aims at enabling efficient and privacy-preserving mutual authentication between mobile users (MUs) and WISPs. User anonymity and identity privacy can be protected, even in the presence of collusion between WISPs and a roaming broker (RB), which is considered to be the strongest user privacy protection. An efficient billing architecture is introduced and performed in the same stage of roaming, where U-tokens are defined and can be purchased by MUs from an RB as authentication credentials for the MUs to access the wireless network. The WISPs, thus, can cash the collected U-tokens in the RB for payment. We show that the proposed authentication and billing architecture can support localized inter-WISP authentication through the divisible blind signature scheme and a local witness strategy. A detailed analysis on a number of performance metrics, such as computation time and power consumption, is given to validate the performance of the proposed architectures.**

***Index Terms*—Billing, partially blind signature, privacy protection, roaming, wireless metropolitan area sharing networks (WMSNs).**

I. Introduction

HIGH-SPEED, low-cost ubiquitous Internet access has been a long-standing vision and has attracted extensive attention from both academia and industry in the past decade. As shown in recent studies, low deployment costs and a high demand for wireless access have led to rapid deployments of public wireless local area networks (WLANs) in densely populated areas such as airports, restaurants, cafes, libraries, and hotels. On the other hand, the deployment of large-scale city-wide broadband Internet access is seriously lagging behind since wireless Internet service providers (WISPs) that rely on the cheaper IEEE 802.11 set of technologies are facing difficulties that limit their coverage to selected hotspots. Thus, to provide ubiquitous wireless access in a metropolitan area, it will be a great strategy to support seamless, efficient, and lightweight interdomain roaming among different WISPs under a well-designed management and coordination architecture to broaden the service coverage of the WISPs by sharing the wireless communication infrastructure with each other. In this paper, we call these networks based on publicly or privately owned wireless Internet access points (APs; supporting either existing Wi-Fi or emerging technologies such as WiMAX) wireless metropolitan area sharing networks (WMSNs). Recent research on WMSNs includes PERM [1], MoB [2], P2PWNC [3], and GIANT [4], as well as metropolitan community groups [5], which focus mostly on the wireless resources sharing relationships among WISP peers and do not address the fundamental issue of controlled access to those networks. By considering the fact that WLAN-enabled phones are now on the market, WMSNs could complement 3G networks to provide global-scale ubiquitous broadband wireless access for mobile users (MUs) in the near future.

One of the key issues in achieving ubiquitous broadband wireless access in emerging WMSNs is the development of a suite of effective handover mechanisms that can realize user authentication and billing with *security assurance, privacy preservation, and low handover latency*. In terms of security assurance, mutual authentication is required. Since an MU may connect to APs owned by different WISPs before and after the handover, the targeted WISP (tWISP) has to authenticate the MU before the service access is granted. Meanwhile, the MU has to authenticate the new network domain to mitigate the threat of malicious impersonation. In terms of user privacy preservation, the user concerns are not only about the disclosure of communication content to the public but about the commercial misuse of their personal data as well. For example, location privacy is among the most critical personal information, and thus, users may prefer to travel incognito [6]. To fulfill user privacy preservation, the WMSNs have to adopt some privacy regulations that enforce WISPs and any roaming broker (RB) to adopt appropriate administrative, technical, and physical security measures [7]. In terms of authentication

Manuscript received February 11, 2008; revised August 4, 2008 and August 11, 2008. First published October 24, 2008; current version published May 11, 2009. This work was supported in part by the Natural Sciences and Engineering Research Council of Canada through a strategic research grant. The review of this paper was coordinated by Dr. L. Chen.

H. Zhu, M. Shi, P.-H. Ho, and X. Shen are with the Center for Wireless Communications, Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: h9zhu@bbcr.uwaterloo.ca; mshi@bbcr.uwaterloo.ca; pinhan@bbcr.uwaterloo.ca; xshen@bbcr.uwaterloo.ca).

X. Lin is with the Faculty of Business and Information Technology, Institute of Technology, University of Ontario, Oshawa, ON L1H 7K4, Canada (e-mail: Xiaodong.Lin@uoit.ca).

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.2008.2007983

delay, it plays a major part in interdomain handover delay. With existing centralized authentication approaches such as those based on EAP/802.1x authentication standard [8], a long authentication delay up to 750–1200 ms may be encountered [9], which is due mostly to the lengthy round trip of signaling from the MU, through the RB, until the home WISP (hWISP) is reached. Such a long end-to-end signaling latency will yield high authentication delay, which is not acceptable for any real-time and interactive service.

To achieve scalable, secure, and efficient authentication and billing, this paper proposes a novel *Privacy Preserving Authentication and Billing* (PPAB) architecture for interdomain roaming in WMSNs. In PPAB, a set of distributed protocols operates under lightweight centralized coordination to authenticate MUs for anonymous access. Such distributed design can help PPAB to achieve *localized authentication*, which is defined as that the authentication is performed between the tWISP and MUs without intervention of any third party (e.g., hWISP and RB). Localized authentication can dramatically reduce the authentication latency and allow the bottleneck and single point of failure found in existing authentication schemes [10]–[12] to be avoided.

One of the most critical components of PPAB is the U-token, which is a universally acceptable security credential that aims at integrating the billing and authentication procedures of MUs in a single step. The U-token is an untraceable, refundable, and double-spending-protected electronic currency, which can be purchased by the MUs from the RB and can serve as authentication credential and a payment method for the MUs to gain access to multiple WISP domains in the WMSNs. The U-token can preserve privacy of MUs through the partially blind digital signature technique, which is a cryptographic tool introduced in [13]. The WISPs can claim their credits by performing offline clearance operations. In addition to the privacy-preserving properties by the U-token, the proposed PPAB architecture has the following two desirable properties.

1) **Localized refund mechanism:** In the context of interdomain roaming, "Refund" is an essential functionality of any token-based authentication scheme since a roaming MU needs to collect its remaining credit before performing a handover and entering into another WISP domain [14]. The proposed PPAB architecture provides a localized refund mechanism through a *lightweight divisible blind signature scheme*, where a withdrawn U-token can be divided into multiple subtokens with smaller values such that the MU can pay the exact amount with some subtokens and keep the other subtokens for future spending. The proposed localized refund mechanism only needs the involvement of the MU and the serving WISP (sWISP) and can therefore significantly reduce the transaction latency and avoid system bottleneck.
2) **Localized double spending detection:** Double spending detection is critical to ensure the security of any token-based authentication scheme. Without double spending detection, an MU can easily initiate a service fraud attack by spending a piece of U-token more than once. To avoid excessive involvement of the RB in every interdomain handover for double spending checks, a localized double spending prevention method is proposed in PPAB based on a *local witness strategy*, where the sWISP takes the role of a local witness for the subtokens of a U-token. Therefore, prior to the handover, the MU requests a commitment from the local witness (i.e., the sWISP), which records the remaining credit of the U-token and all the spent subtokens. During the interdomain handover authentication, the MU submits its U-token and the remaining subtokens along with the commitment to the tWISP, which can easily ensure the freshness of the subtokens by verifying this commitment without intervention of any third party.

With the localized refund and double spending detection mechanisms, localized authentication and billing can be achieved under the PPAB architecture. To the best of our knowledge, this is the first study on the issues of localized authentication, billing, and privacy in the context of interdomain roaming in the WMSNs. We will demonstrate that the proposed architecture is highly energy and computation efficient.

The remainder of this paper is organized as follows. In Section II, a brief overview of related work is presented. Section III introduces the system model and design goals. In Section IV, the proposed PPAB architecture is presented. The security of the PPAB architecture is analyzed and discussed in Section V, followed by the efficiency analysis in Section VI. Finally, Section VII concludes this paper.

II. Related Work

Nowadays, there is no established standard for roaming between WISPs. There are two interdomain roaming models applicable to multi-WISP roaming: 1) *bilateral* model and 2) *broker/aggregator* model [15]. The bilateral model requires that the hWISP should have a bilateral contractual agreement with the foreign WISP. This model works well in the cellular networks because of the limited number of cellular providers, while it may not be suitable in the WMSN application scenario due to a much larger number of WISPs [11]. In addition to the bilateral model, an alternative can be such that roaming is performed by way of having an RB [16] trusted by all the WISPs to facilitate the peer-to-peer wireless resources sharing among different WISPs. This approach has attracted extensive attention from both academia (i.e., PERM [1], MoB [2], P2PWNC [3], and GIANT [4]) and industry (i.e., AbitCool [17] and Fon [18]) due to its good scalability and flexibility. They focus mostly on stimulating wireless resources sharing among different WISPs and do not address the fundamental issue of interdomain authentication and billing issue.

On the other hand, existing authentication approaches such as those based on the 802.1x standard [8] are ill-suited for the WMSNs since it inevitably runs the risk of making the RB to become the bottleneck in the inter-WISP roaming and authentication request processing. In addition, the entire authentication process using the 802.1x method involves several rounds of communication between the MU, the RB, and the hWISP, which leads to high and variable delay. However, low

authentication delay is critical for supporting emerging real-time service applications and seamless handoffs.

To reduce authentication delay, a number of fast authentication schemes have been reported for seamless handovers in situations where an MU roams between adjacent APs under a common WISP domain (also referred to as intradomain handover), such as predictive authentication [19], pre key distributions [20], and enhanced inter-AP protocol (IAPP) [21]. However, these schemes mainly rely on the RB to predistribute the handover keys or preprocess the authentication requests, which may impose a heavy burden on the RB. On the other hand, *localized authentication*, which aims at localizing the authentication process between the tWISP and MUs without contacting the hWISP and the RB, created a new paradigm toward shortening the authentication delay and reducing the load on the RB [22]. In [23] and [24], it is suggested that a local AAA server be used as a buffer for caching the security contexts for each active MU. This scheme can greatly improve the performance since an MU requesting for handoff needs to communicate with the home AAA server only for once, and then, the subsequent authentication procedure can be performed at a local AAA server. Although the scheme is intuitive and effective, it cannot provide a seamless interdomain handover for those roaming MUs that did not visit the wireless domain before. Another typical localized authentication method is by way of some long-term security credential (e.g., a public key certificate issued by the RB) to avoid real-time interaction with the RB and hWISP [4], [10]–[12]. These schemes are secure, scalable, and efficient, at the expense of infringing of user anonymity, where the RB is allowed to track spending and/or location information of MUs.

Other approaches that have addressed the issue for WISPs to provide wireless access to each other's MUs include reputation-based solutions [25] and exchange-based incentive mechanisms [26]. These proposals have focused on providing incentives for sharing of wireless communication resources among different WISPs, while they do not take authentication delay and privacy issues into consideration. The studies that are most closely related to the proposed PPAB architecture are in the class of E-cash-based authentication schemes [27]–[30]. These schemes take advantage of blind signatures as the authentication credential to provide anonymity and unlinkability for the user authentication and billing. However, none of these schemes have specifically considered the interdomain handover issues. Note that one of the unique features for the interdomain handover in the WMSNs lies in the fact that an MU needs to collect the remaining credit before the handover and should be seamless authenticated after the handover with minimal delay.

III. System Model and Design Goal

In this section, the system model and security requirements are presented.

A. System Model

We assume that the WMSN is composed of numerous IEEE 802.11-based wireless routers. A number of wireless network domains exist, and each is managed by an independent WISP. With PPAB, three players exist in the WMSN, namely, 1) WISPs, 2) MUs, and 3) the trusted RB. Similar to previously reported RB-based roaming architectures such as [22], each WISP only needs to have an agreement with the RB instead of a pairwise bilateral trust relationship with the other WISPs. PPAB is based on the conventional public key infrastructure in building the trust relationship among different WISPs and between WISPs and MUs. In addition, the RB can also serve as a certificate authority and issue a corresponding certificate to every legitimate WISP such that each WISP can check the validity of the others. We assume that a legitimate WISP does not intentionally misbehave, which is reasonable since the attacks on its MUs will decrease the satisfactory of the MUs on the WISP and will lead to a reduction in its long-term revenue. On the other hand, the attacks launched by a WISP can easily be detected by the RB, and the malicious WISP will be deprived of its WISP qualification with subsequent penalties. Furthermore, we assume that the revocation event for a WISP is rare; thus, it is reasonable for the RB to update in real time and distribute the certificate revocation list of the WISPs.

B. Design Goals

To ensure privacy-preserving authentication and billing, the following security requirements are considered.

1) **Mutual authentication and key agreement**: The MU and the tWISP should be two-way (or mutually) authenticated during an interdomain handover event, by which a fresh session key should be generated to protect the security of communication channel between the MU and the WISP.
2) **Privacy preserving**: Five levels of privacy protection are defined as follows:
   a) *content privacy*: hiding communication content from the external attackers;
   b) *external privacy*: hiding identity information of MUs from the external attackers;
   c) *internal privacy I*: hiding identity information of MUs from the WISPs;
   d) *internal privacy II*: hiding identity information of MUs from the RB;
   e) *internal privacy III*: hiding identity information of MUs from attackers (including both of external attackers and internal attackers) for each communication session (or named *intersession unlinkability*) or each handoff event (or named *inter-handoff unlinkability*.)

   Note that in an interdomain handoff event, to keep the traffic undisrupted, the mapping relationship of MUs' previous identity and current identity used in the sWISP and tWISP domains, respectively, should be available to the tWISP. Otherwise, the packets, which are intercepted by the previous WISP, tunneled to the current WISP, and destined for the MU, cannot be successfully delivered to the MUs due to the lack of destination information. This makes inter-handoff unlinkability unsuitable for realizing a seamless interdomain handoff,

although from the traditional cryptographical point of view, inter-handoff unlinkability can provide stronger privacy-preserving functionality. Thus, we consider intersession unlinkability as the highest privacy-preserving requirement in this paper. We name a system that can achieve the above five level privacy protection requirements as a *perfect anonymity/privacy*-preserving system. In some other application scenarios such as emergencies or criminal behavior investigation, where the legal authorities should be able to reveal the real identity of a U-token holder, "revocable privacy" may be a suitable alternative to make a balance between the privacy preserving and information auditing. The PPAB architecture can easily be extended to provide revocable privacy by adopting the fair blind signature technique [31], which is out of the scope of this paper.

3) **Nonrepudiated billing**: When an MU roams among different WISPs, he/she could be wrongly charged due to a billing error or security breach by the sWISP. Nonrepudiated billing is a security service that provides evidence to enable the settlement of disputes over usage fees.

In addition to the above security goals, the proposed architecture should also include the following efficiency goals: 1) *Low authentication latency*: The proposed authentication and billing architecture should minimize the authentication delay. 2) *Scalability*: The proposed architecture should avoid any bottleneck and single point of failure.

C. Cryptographic Preliminaries

The proposed PPAB architecture is based on two cryptographic techniques, namely 1) the partially blind signature and 2) Rabin's public key cryptosystem. A brief review of the two techniques is given as follows.

1) Divisible Partially Blind Signature: A blind signature is a kind of digital signature in which the content of a message is disguised from its signature. The blind signature technique has been widely used due to its distinct property of unlinkability (or blindness) property, particularly in services that emphasize user privacy, such as anonymous electronic voting, electronic cash (E-cash), and notary public services. A blind signature scheme with the unlinkability property was first introduced in [32]. It is a cryptographic primitive that involves two entities, namely: 1) a signer and 2) a signature requester. The cryptographic primitive allows the requester to have the message signed by the signer without revealing any information about the message. With a secure blind signature scheme, the signer is unable to link (or trace) the signed message to the previous signing process, where the requester cannot be traced while using the signed message.

Two issues should be considered when applying the blind signature technique in the proposed PPAB architecture. First, due to lack of control over the messages to be signed, it takes extra effort to include denomination and/or expiry information in the blind signature by using a partially blind signature [33]. The partially blind signature scheme allows the signer to produce a blind signature on the message for the recipient, and the signature explicitly includes some common agreed information that remains clearly visible despite the blinding process. With the partially blind signature applied in PPAB, expiry date and denominational information can be embedded in U-tokens, which is necessary in the interdomain handover procedure. Another issue is on providing an efficient refund mechanism for MUs. An efficient refund mechanism should be subject to the following properties: 1) The refunded credit should be reusable as payment in the future consumption of Internet services, and 2) the overhead in receiving refund credit should be minimal. The divisible blind signature scheme is a concept that could support refund functionality for a blind-signature-based E-cash system, where every E-cash can be divided into multiple subcash denominations of smaller values such that the exact payment can be supported. In PPAB, we propose an efficient divisible partially blind signature by seamless integrating the partially blind signature scheme and the hash chain technique, which will be detailed in Section IV-B.

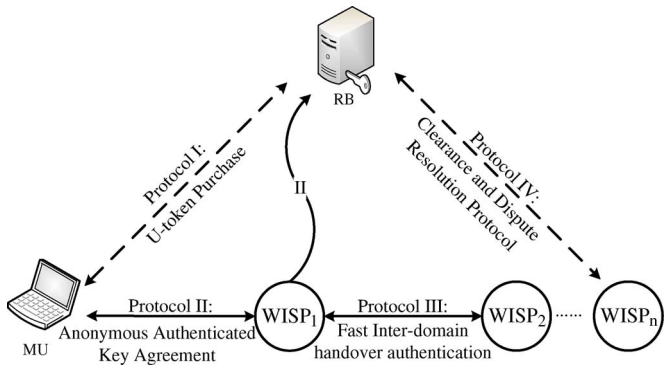


Fig. 1. Overview of PPAB protocols.

2) Rabin's Public Key Cryptosystem: Rabin's public key cryptosystem serves as the cryptographic foundation in our work [34], which is based on the large number factorization problems. The Rabin's scheme is notably characterized by its asymmetric computational cost, where the decryption (or signature verification) operation is extremely fast, while the encryption (or signature signing) operation is comparably slow and requires a large amount of computation effort [35]. This great property makes Rabin's scheme very suitable in a heterogeneous wireless network environment such as WLANs or WMSNs, in which an AP has a very large computational capacity, while the mobile stations of MUs are subject to stringent resource limitation. With Rabin's scheme, an authenticated key agreement scheme can be developed such that the cryptographic burden can be properly allocated across the network entities in WLANs or WMSNs. The PPAB architecture is designed based on Rabin's public key cryptosystem, which aims at greatly reducing the computational overhead in the MU side at the expense of putting more load on the AP [13].

IV. Proposed Privacy-Preserving Authentication and Billing Architecture

As shown in Fig. 1, the proposed PPAB architecture works as follows: in "Protocol 0: System Initialization Protocol," the RB chooses its public/private key pairs and generates public

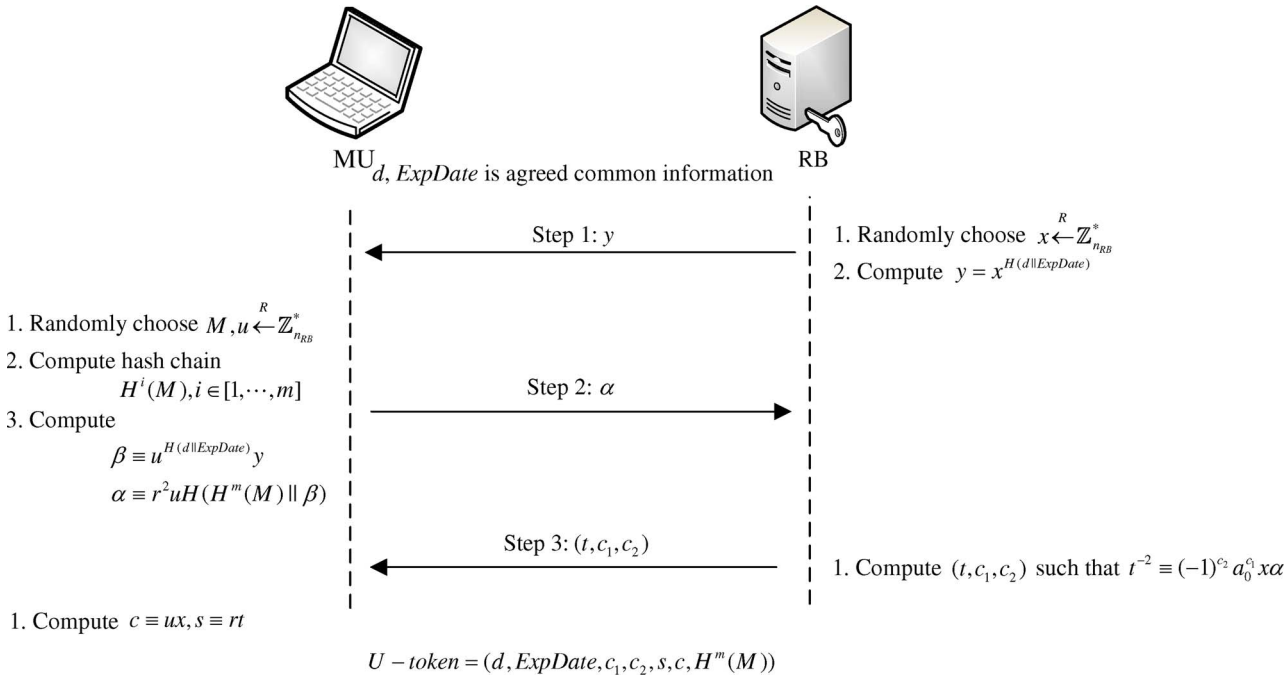


Fig. 2. U-token purchase protocol.

key certificate for every WISP. An MU obtains a U-token from the RB through "Protocol I: U-token Purchase Protocol." Then, the MU uses the U-token to access to the network through any desired WISP, where mutual authentication and key agreement are performed without disclosure of the MU's context information by invoking "Protocol II: Anonymous Authenticated Key Agreement Protocol." Note that since it is the first access of MUs when the real-time service has not been initialized, PPAB allows the double spending check of U-tokens to be performed under the help of the RB. To avoid the necessity of contacting the RB for a U-token double spending check in the subsequent consecutive interdomain handoff, the proposed PPAB architecture localizes the double spending check by a local witness strategy, which is detailed in "Protocol III: Fast Inter-domain Handover Authentication Protocol." Finally, "Protocol IV: Clearance and Dispute Resolution Protocol" is developed to perform clearance of a U-token and resolve possible disputes that might rise among the MUs, the WISPs, and the RB. It is important to point out that only Protocols II and III are performed on-line, while the others are conducted off-line for the maintenance or preparation of the future handoff events.

A. System Initialization Protocol

The RB randomly chooses two primes p_{RB} and q_{RB} as the private keys, where p_{RB}, $q_{\mathrm{RB}} \equiv 3 (\mathrm{mod}\ 4)$. The triplet $(a_0, n_{\mathrm{RB}}, a_0^{-1})$, together with one hash function H, are published as the public key, where $n_{\mathrm{RB}} = p_{\mathrm{RB}} \cdot q_{\mathrm{RB}}$, and a_0 satisfies the Jacobi symbol $(a_0/n_{\mathrm{RB}}) = -1$. Similarly, for WISP A, which is going to join this trust domain, it chooses its private key p_A, q_A and public key $n_A = p_A \cdot q_A$ following the same way as that by the RB. Then, WISP obtains a public key certificate that binds A's identity (denoted as ID_A) to its public key $PK_A = \langle ID_A, n_A, ExpDate \rangle$ through the signature signed by the RB, where $ExpDate$ is the validity period defined for A.

B. U-Token Purchase Protocol

The proposed PPAB architecture is based on the exchange of U-tokens, which takes advantage of the blind signature to hide the association between the security credential and the MU's real identity. To provide refundable property, PPAB integrates the one-way hash chain technique [36] with the partially blind signature scheme to come up with a lightweight divisible partially blind signature mechanism. As shown in Fig. 2, the detailed U-token purchasing protocol is described as follows.

Step 1: Let d be the face value of the U-token that an MU is requesting, and let $ExpDate$ refer to the expiration date of the U-token. The RB generates one fresh nonce $x \in Z^*_{n_{\mathrm{RB}}}$ as the randomizing factor and sends y to the MU, where $y = x^{H(d\|ExpDate)} (\mathrm{mod}\ n_{\mathrm{RB}})$.

Step 2: Based on the face value of the U-token d, the MU selects a random integer m and generates a one-way hash chain $H^m(M) = H(H(\cdots(H(M)\cdots)))$ by applying a one-way function $H()$ to M for m times, where every hash token $H^i(M)$, $i \in [1, \ldots, m]$, stands for a monetary value τ such that $d = m \times \tau$. After receiving the commitment value y, the MU also selects its randomizing factor $u \in Z^*_{n_{\mathrm{RB}}}$ and computes $\beta \equiv u^{H(d\|ExpDate)} y (\mathrm{mod}\ n_{\mathrm{RB}})$. The MU then selects the blinding factor $r \in Z^*_{n_{\mathrm{RB}}}$ for computing the blinded message submitted to the RB: $\alpha \equiv r^2 u H(H^m(M)\|\beta) (\mathrm{mod}\ n_{\mathrm{RB}})$.

Step 3: After receiving α, the RB injects its randomizing factor x into the blinded message α and computes (t, c_1, c_2), which satisfies the relationship

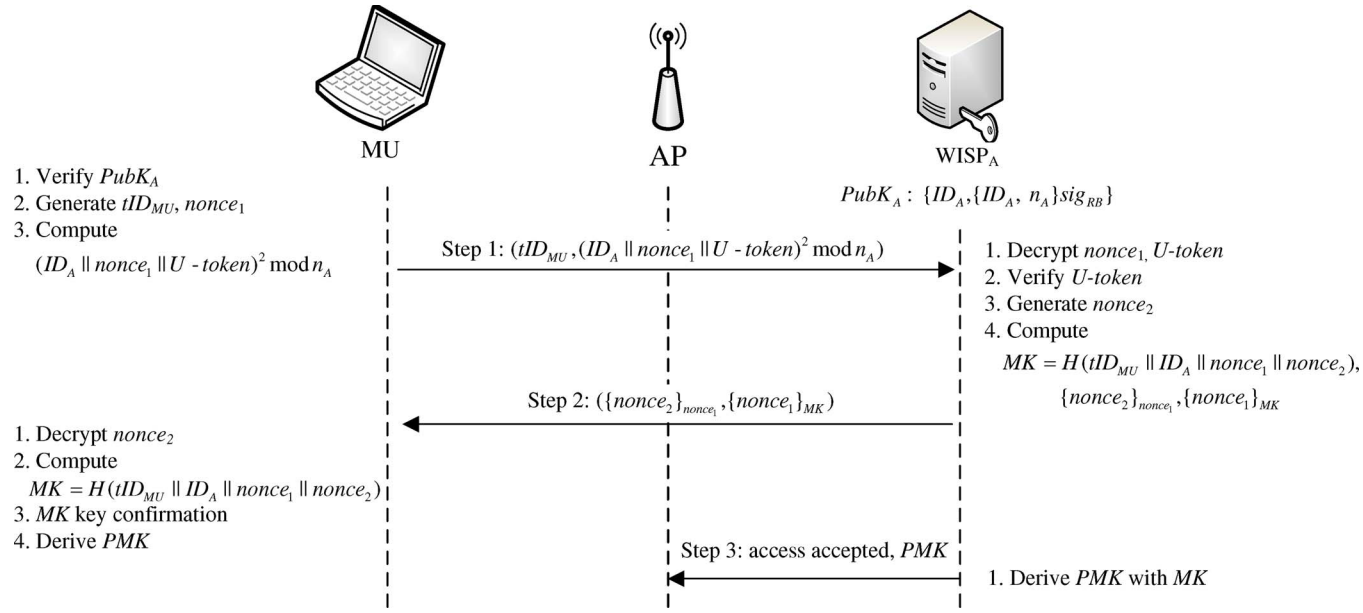


Fig. 3. Anonymous authenticated key agreement protocol.

$t^{-2} \equiv (-1)^{c_2} a_0^{c_1} x\alpha (\mathrm{mod}\ n_{\mathrm{RB}})$. Here, c_1 can be computed in the following fashion:

$$c_1 = \begin{cases} 0, & \text{if } \left(\frac{x\alpha}{n_{\mathrm{RB}}}\right) = 1 \\ 1, & \text{if } \left(\frac{x\alpha}{n_{\mathrm{RB}}}\right) = -1 \end{cases}$$

and then, the RB computes $\beta = a_0^{c_1} \cdot x\alpha (\mathrm{mod}\ n_{\mathrm{RB}})$ and derives c_2 such that

$$c_2 = \begin{cases} 0, & \text{if } \left(\frac{\beta}{p_{\mathrm{RB}}}\right) = \left(\frac{\beta}{q_{\mathrm{RB}}}\right) = 1 \\ 1, & \text{if } \left(\frac{\beta}{p_{\mathrm{RB}}}\right) = \left(\frac{\beta}{q_{\mathrm{RB}}}\right) = -1. \end{cases}$$

Then, the RB can derive t such that $t^{-2} \equiv (-1)^{c_2} a_0^{c_1} x\alpha (\mathrm{mod}\ n_{\mathrm{RB}})$. Here, we follow a standard improved Rabin's signature to derive (t, c_1, c_2) [34]. The blinded signature (t, c_1, c_2) and the randomizing factor x are sent to the MU.

Step 4: The MU computes $c \equiv ux (\mathrm{mod}\ n_{\mathrm{RB}})$ and $s \equiv rt (\mathrm{mod}\ n_{\mathrm{RB}})$ and obtains a full U-token $(d, ExpDate, c_1, c_2, s, c, H^m(M))$.

Note that a full U-token is comprised of the following two parts: 1) $(d, ExpDate, c_1, c_2, s, c, H^m(M))$, which is a typical partially blind signature based on the improved Rabin's scheme; and 2) $H^i(M), i \in [1, \ldots, m]$, which divides an original blind signature of face value d into m subtokens. The value of each piece of subtoken is τ. The validation of U-token $= (d, ExpDate, c_1, c_2, s, c, H^m(M))$ can be examined by verifying the following congruence:

$$s^2 H\left(H^m(M) \| c^{H(d \| ExpDate)} (\mathrm{mod}\ n_{\mathrm{RB}})\right) c \equiv (-1)^{c_2} a_0^{-c_1} (\mathrm{mod}\ n_{\mathrm{RB}}). \quad (1)$$

A detailed security analysis of the proposed U-token issuing mechanism will be discussed in Section V.

C. Anonymous Authenticated Key Agreement Protocol

After submitting the U-token, the MU can gain access to any available wireless network operated by a WISP, accepting the U-token as a valid payment method. Let A denote the local authentication server of tWISP. As shown in Fig. 3, the detailed access process is described as follows.

Step 1: Let A periodically broadcast its public key certificate $(PubK_A)$ along with a service set identifier (SSID). The MU can easily authenticate A by validating $PubK_A$. To keep the freshness of the agreed key, the MU chooses a random integer $nonce_1$ as the key contribution, which will be employed to derive the future shared key, and another random integer tID_{MU} as its temporal identity. After that, the MU encrypts $nonce_1$ with ID_A's public key by using the relation

$$(ID_A \| nonce_1 \| U - token)^2 (\mathrm{mod}\ n_A).$$

Note that the encryption follows a standard Rabin's encryption scheme, which is extremely efficient as it only involves a single modular squaring. Then, the MU sends it as well as tID_{MU} to A.

Step 2: After decrypting the encrypted message and obtaining $nonce_1$ and the U-token, A ensures the validity of the U-token through the following steps.

a) Verify the validity of U-token by checking (1).
b) Check if this U-token expires.
c) Search in the RB's database to check whether this U-token has been spent before. If negative, the RB will record this U-token for future check.

If these three conditions are satisfied, A accepts the MU as a legitimate user and then selects a fresh nonce $nonce_2$ as A's key contribution. The master key MK between the MU and A can be derived as

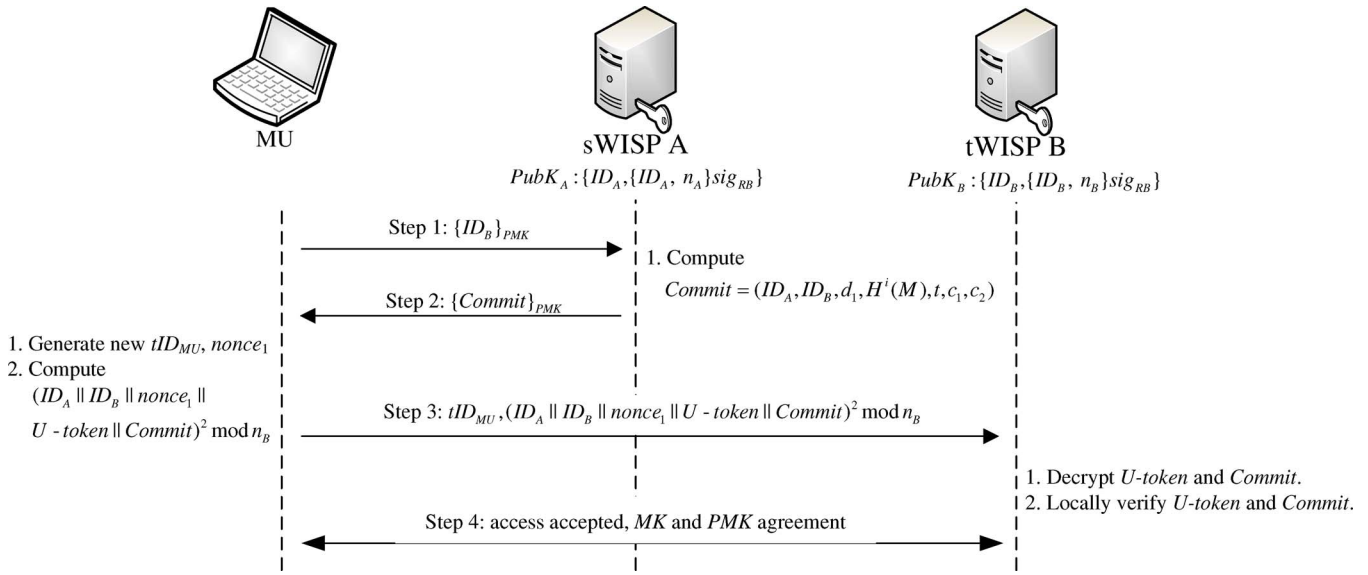


Fig. 4. Fast interdomain handover-authentication protocol.

$MK = H(tID_{\mathrm{MU}} \| ID_A \| nonce_1 \| nonce_2)$. Then, A sends encrypted $\{nonce_2\}_{nonce_1}$ as well as the key confirmation $\{nonce_1\}_{MK}$ to the MU.

Step 3) The MU obtains $nonce_2$ by using symmetric-key decryption and computes the master key $MK = H(tID_{\mathrm{MU}} \| ID_A \| nonce_1 \| nonce_2)$. According to the IEEE 802.11i authentication framework, a master key MK can be used to derive a pairwise master key (PMK). The authentication server securely delivers this PMK key to the AP. Then, the MU and the AP can use the PMK to authenticate each other and perform the four-way handshake protocol to derive the pairwise transient key and group transient key to secure the transmission channel between the MU and the AP.

After completing the above authentication protocols, the MU and WISP have successfully authenticated each other without revealing the real identity of the MU. After that, the MU will be charged according to the consumed wireless service. To enable the interdomain payment to be performed in a secure and incontestable way, the idea of micropayment [36] is exercised to maintain a secure communication session, by which the MUs are forced to periodically submit a subtoken to maintain the session consistency. More specifically, when the amount of spending of the MU is equal to τ money units, it triggers the submission of the first subtoken $ST_1 = H^{m-1}(M)$, which is sent by the MU to its serving AP. The AP can check the validity of this proof by simply verifying if $H(ST_1) = H^m(M)$ holds. The above-described procedure can be repeated until the roaming credit of this MU has run out, or the MU is going to make a handover.

Note that in the above anonymous authenticated key agreement protocol, the WISPs still need to contact the RB for U-token double spending detection and U-token deposit. Here, we still follow the traditional centralized way to prevent double spending checking. Although it introduces extra network latency, we argue that the latency is acceptable since it is the first time for the MU to gain access from the Internet, and thus, no real-time applications have been started. However, in subsequent interdomain handover events, handover delay has to be minimized to support real-time traffic. In Section IV-D, a local witness strategy that can localize the double spending check operations will be discussed in detail.

D. Fast Interdomain Handover-Authentication Protocol

An interdomain handover event switches an active communication session from an AP of the original serving domain to another AP with a different managing WISP. As discussed before, how the double spending check operation is localized without contacting the RB is a critical design in the proposed PPAB architecture. Here, we adopt the "witness" approach to design a localized U-token double spending checking operation.

A witness approach was first proposed in [37] to ensure real-time double spending prevention of electronic coin systems without the participation of any centralized on-line trust party. The basic idea of the witness approach is that every electronic coin is randomly assigned to one of the receiver peers, who will serve as a witness for validity of that coin. In this paper, we further extend the witness approach to the scenario of *local witness*, which is motivated by the fact that the sWISP, which has accepted the U-token and some of the subtokens, can naturally be the "witness" of this U-token to provide a "freshness" proof for the tWISP. Thus, prior to the handover, the MU can request a remaining credit commitment from the sWISP. This commitment will be submitted along with the original U-token to the tWISP in case the authentication for interdomain roaming is performed.

The proposed Fast Inter-domain Handover Authentication Protocol is illustrated in Fig. 4 and will be further detailed in the following paragraphs.

Step 1: The MU sends a handover request to A, indicating that the MU intends to roam into B.

Step 2: Upon receiving the handover request from the MU, A checks the identity of B by verifying its public key certificate. If verification passes, A summarizes the MU's remaining credits d_1 and generates a commitment for the MU. Such a commitment is a public verifiable proof about the remaining credit of U-token and all the spent subtokens. Supposed that the last spent subtoken is $H^i(M)$, A computes (t, c_1, c_2) such that $t^2 \equiv (-1)^{c_2} \cdot a_0^{c_1} H(ID_A \| ID_B \| d_1 \| U-token \| H^i(M))$. Here, we follow a standard improved Rabin signature scheme to obtain (t, c_1, c_2). Then, A sends the commitment $\mathbf{Commit}_1 = (ID_A, ID_B, d_1, H^i(M), t, c_1, c_2)$ to the MU.

Step 3: After receiving $\mathbf{Commit}_1$, the MU obtains its refund $(U-token, \mathbf{Commit}_1, H^{i+1}(M), \ldots, H^m(M))$, where $(H^{i+1}(M), \ldots, H^m(M))$ is the remaining credit of the MU. Such a refund mechanism is localized since it is executed between the sWISP and the MU without the intervention of the RB. Afterward, the MU simply follows the standard authenticated key agreement protocol defined in Section IV-C to roam into network domain B with the U-token as well as commitment.

Step 4: B verifies the RB's signature on the U-token and the correctness of the commitment. Since this commitment is valid only for B, the whole verification process can be performed locally without the intervention of the RB, where localized authentication for inter-WISP roaming can be achieved. With this, the MU and the $tWISP$ obtain the MK and PMK similar to that defined in Section IV-C.

It is important to point out that PPAB differs from the conventional token-based approach in that PPAB can support an MU to reuse a U-token at multiple WISPs. When a U-token is first used, the U-token should be deposited at the RB, which can be seen as the registration phase. However, when the remaining credits of this U-token is used at the second or other WISP, the freshness of a U-token is determined not only by the original U-token but also by the subtokens and commitment. For example, in the subsequent kth interdomain handover event, the WISP k generates the new $\mathbf{Commit}_k = (ID_k, ID_{k+1}, d_k, H^{i_k}(M), t_k, c_{k_1}, c_{k_2})$ such that

$$t_k^2 \equiv (-1)^{c_{k_2}} \cdot a_0^{c_{k_1}} H\left(ID_k \| ID_{k+1} \| d_k \| \text{U-token} \| H^{i_k}(M)\right)$$

where ID_k and ID_{k+1} denote the sWISP and tWISP, respectively, d_k denotes the remaining credit after handoff from WISP k, and $H^{i_k}(M)$ denotes the latest spent subtoken. With $\mathbf{Commit}_k$ as well as U-token and subtokens, MU can do a seamless handover to the next WISP. The above-described procedure can be repeated until the roaming credits of this MU has run out, or the MU is going to finish the interdomain roaming by logging off. Before logging off, to collect the remaining credits, the MU can obtain a new U-token by performing another U-token purchase protocol described in Section IV-B.

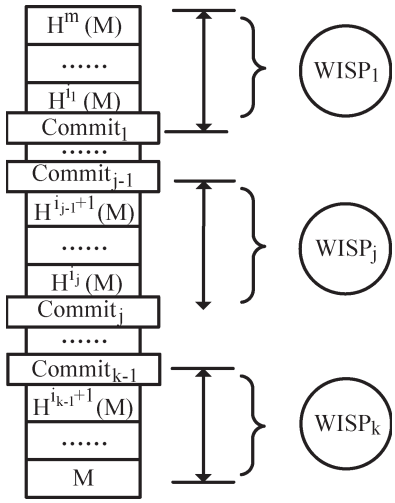


Fig. 5. Clearance example.

E. Clearance and Dispute-Resolution Protocol

With the proposed PPAB architecture, the RB also serves as an automated clearing house to make the inter-WISP payment perform efficiently. In the clearance phase, the WISP submits the U-tokens, i.e., $\mathbf{Commit}$, and the corresponding subtokens to the RB for verification. Note that with PPAB, the credit gained by the WISP in the clearance is determined by the denomination of the collected subtokens rather than the original U-tokens. An example is given in Fig. 5, where an MU roams among k different WISP domains, and every WISP has received a subtoken block. For WISP j, its subtoken block ranges from $ST_{i_{j-1}+1} = H^{i_{j-1}+1}(M)$ to $ST_{i_j} = H^{i_j}(M)$, where i_{j-1} and i_j refer to the index of the last subtoken received by WISP $j-1$ and WISP j, respectively. Therefore, before crediting this WISP, the RB checks in its database to see if this U-token has already been deposited. In the example, this U-token is first used by WISP 1, and therefore, the RB will give WISP 1 credits in accordance with the collected subtokens. Otherwise, the RB will check the correctness of commitment at first and then calculate the credits of the WISP based on the subtokens. As for WISP j, which submitted the original U-token, i.e., $\mathbf{Commit}_{j-1} = (ID_{j-1}, ID_j, d_j, H^{i_{j-1}}(M), t_{j-1}, c_{j-1_1}, c_{j-1_2})$, and collected subtokens $ST_l = H^l(M)$, $i_{j-1} + 1 \le l \le i_j$ for clearance, the RB will perform the following steps to credit WISP j.

1) Verify $\mathbf{Commit}_{j-1}$ by checking if ${t_{j-1}}^2 \equiv (-1)^{c_{j-1_2}} \cdot a_0^{c_{j-1_1}} H(ID_{j-1} \| ID_j \| d_{j-1} \| \text{U-token} \| H^{i_{j-1}}(M))$ holds.
2) Verify the subtokens by checking if $ST_l = H(ST_{l-1})$, $l \in \{i_{j-1}+1, \ldots, i_j\}$.
3) Calculate the corresponding credit of WISP j by computing $Cre = (i_j - i_{j-1}) \times \tau$. Then, WISP j will be credited for Cre.

The possible dispute events can be categorized into the following two classes: 1) a dispute between MU and WISP and 2) a dispute among WISPs. In 1), since a hash-chain-based micropayment method is adopted, PPAB presents no credit loss risk to an MU. In 2), the credit of WISP k is bounded by $\mathbf{Commit}_{k-1}$ and $\mathbf{Commit}_k$. Therefore, although WISP k can derive the subtokens held by MU's previous visit to WISP, such

as WISP $k-1$, it is still impossible for WISP k to overclaim its credit since it cannot forge another $\mathbf{Commit}_{k-1}$.

F. Discussions

1) Load on the RB: The major load on the RB is the cost incurred by U-token issuing, storing, and searching (double spending detection). As for U-token issuing cost, the localized refund design of PPAB relieves the RB from the involvement in every interdomain handoff event, and an MU can gain access to multiple WISP domains during the continuous interdomain handoff events with a single U-token. Therefore, the RB's involvement is reduced from $O(\mathcal{MN})$ to $O(\mathcal{M})$, where $\mathcal{M}$ is the number of U-token issued, $\mathcal{N}$ is the average number of interdomain handoffs occurring during the life time of a U-token, and thus, $O(\mathcal{MN})$ is total number of interdomain handoff events within the whole WMSN. For a large-scale WMSN that contains numerous independent WISPs with frequent interdomain handoff events, PPAB will dramatically reduce the load on the RB. Further, PPAB takes advantage of the partially blind signature technique to keep the size of the U-token storing database under control. By embedding the expiration date into each U-token, all the corresponding records of the expired U-token in the bank database can thus be removed. In other words, the database of the RB only needs to keep the unexpired U-tokens deposited by the MUs to prevent double spending. Such design can further reduce the storing and searching cost incurred by the U-token double spending detection.

2) Trust Relationship: In addition to trust relationship with the RB, PPAB localizes double spending detection based on the "local witness" approach, which requires the tWISP "trusts" the commitment issued by sWISP as the freshness proof. However, different from the bilateral roaming model, which requires that each pair of WISPs should establish the peer-to-peer trust relationship, the trust relationship between the WISPs in PPAB only exists among neighboring WISPs since an MU can only hand off from sWISP to the neighboring WISPs. Because the number of neighboring WISPs may be orders of magnitude lower than the total number of WISPs, PPAB is more scalable and flexible than the bilateral model.

3) Witness Motivation: As a general answer to the motivation issue of the "witness" approach, Osipkov *et al.* [37] pointed out that preventing double spending helps the community as a whole, and most of the peers would, in general, be willing to do a little extra work to contribute to the health of the community. It is further suggested that the RB can provide incentives to witness for generating commitment. In PPAB, it is worth pointing out that the witness approach can localize the authentication and billing process. This is particularly beneficial for reducing interdomain handoff authentication signaling overhead and latency and meeting the increased demand on seamless roaming of MUs. The increased satisfactory of MUs, in turn, will benefit the WISPs for a long time, which can be another motivation for our "local witness" strategy.

V. Security Analysis

The security of the proposed architecture relies on the security of U-token, which is essentially a partially blind signature. We analyze the security issues related to the U-token, including correctness, untraceability, and unforgeability. After that, the security properties of the proposed PPAB scheme are studied.

A. Security Characteristics of U-Token

According to [13], a blind-signature-based U-token scheme should satisfy the following security requirements.

1) Correctness: According to the following theorem, we ensure that the proposed U-token (partially blind signature) is correct.

Theorem 1: If $(d, ExpDate, c_1, c_2, s, c, H^m(M))$ is a U-token formed by both the RB and the MU according to the steps defined in Section IV-B, then

$$s^2 H(H^m(M)\|c^{H(d\|ExpDate)} \bmod n_{\mathrm{RB}})c \equiv (-1)^{c_2} a_0^{-c_1} (\bmod\ n_{\mathrm{RB}})$$

holds.

Proof: We have

$$\begin{aligned}
&s^2 H\left(H^m(M)\|c^{H(d\|ExpDate)} \bmod n_{\mathrm{RB}}\right) c \\
&\quad \equiv (rt)^2 H\left(H^m(M)\|c^{H(d\|ExpDate)} \bmod n_{\mathrm{RB}}\right) ux \\
&\quad \equiv r^2 t^2 uxH\left(H^m(M)0\|c^{H(d\|ExpDate)} \bmod n_{\mathrm{RB}}\right) \\
&\quad \equiv r^2 \left((-1)^{c_2} a_0^{c_1} \alpha x\right)^{-1} uxH \\
&\qquad \times \left(H^m(M)\|c^{H(d\|ExpDate)} \bmod n_{\mathrm{RB}}\right) \\
&\quad \equiv r^2 \Big((-1)^{c_2} a_0^{c_1} r^2 uxH \\
&\qquad\quad \times \left(H^m(M)\|c^{H(d\|ExpDate)} \bmod n_{\mathrm{RB}}\right)\Big)^{-1} \\
&\qquad \times uxH\left(H^m(M)\|c^{H(d\|ExpDate)} \bmod n_{\mathrm{RB}}\right) \\
&\quad \equiv (-1)^{c_2} {a_0}^{-c_1} (\bmod\ n_{\mathrm{RB}}).
\end{aligned}$$

2) Unlinkability (Blindness) of the U-Token: Suppose that a U-token $(d, ExpDate, c_1, c_2, s, c, H^m(M))$ is the ith U-token issued by an RB, the RB can record (α_i, x_i, t_i) obtained from the U-token issuing process. The triplet (α_i, x_i, t_i) is referred as the *view* of the RB upon the instance i, which is stored by the RB for tracing the identity of MUs in the future. However, with the unlinkability property, the RB cannot derive a link between the *view* and a valid U-token after the MU spends the U-token on a WISP, which remits this U-token to the RB. Without this property, the RB can learn about the user's identity by linking the U-token to a specific view, and the MU's context information may be known by the RB, which obviously infringes the users' privacy. Theorem 2 ensures the unlinkability property of the scheme.

Theorem 2: Given a U-token $(d, ExpDate, c_1, c_2, s, c, H^m(M))$ produced by the proposed scheme with common information d and $ExpDate$, the RB can derive u and r for each view (α_i, x_i, t_i) such that the following three relations are satisfied:

$$c \equiv ux_i (\bmod\ n_{\mathrm{RB}}) \tag{2}$$

$$\alpha_i \equiv r^2 uH\left(H^m(M)\|c^{H(d\|ExpDate)} \bmod n_{\mathrm{RB}}\right) \tag{3}$$

$$s \equiv rt_i (\bmod\ n_{\mathrm{RB}}). \tag{4}$$

The above relations imply that all the U-tokens are indistinguishable from the RB's point of view.

Proof: With PPAB, a U-token $(d, ExpDate, c_1, c_2, s, c, H(m))$ and a piece of *view* (α_i, x_i, t_i) can explicitly determine $H(H^m(M)\|c^{H(d\|ExpDate)} \bmod n_{\mathrm{RB}})$. With x_i and c, the RB can derive the integer u by computing

$$u = cx_i^{-1} (\bmod\ n_{\mathrm{RB}}) \tag{5}$$

from (2).

With the derived u, α_i, and (3), the signer can obtain a determined r with the knowledge of factoring of n_{RB} by computing

$$r \equiv \left(\alpha_i \left(uH\left(H^m(M)\|c^{H(d\|ExpDate)} \bmod n_{\mathrm{RB}}\right)\right)^{-1}\right)^{1/2}. \tag{6}$$

Since the U-token $(d, ExpDate, c_1, c_2, s, c, H(m))$ is produced according to the proposed partially blind signature scheme, (1) must hold, which leads to

$$s \equiv \left((-1)^{c_2} a_0^{-c_1} \left(H\left(H^m(M)\|c^{H(d\|ExpDate)} \times \bmod n_{\mathrm{RB}}\right)c\right)^{-1}\right)^{1/2} (\bmod\ n_{\mathrm{RB}}). \tag{7}$$

Furthermore, from the stored view, we can obtain t, which satisfies $t_i = ((-1)^{c_2} a_0^{c_1} x_i \alpha_i)^{-1/2}$. Next, we show that (4) is also satisfied for the determined integers r, s, and t_i by

$$\begin{aligned} rt_i &\equiv \left(\alpha_i \left(uH\left(H^m(M)\|c^{H(d\|ExpDate)} \bmod n_{\mathrm{RB}}\right)\right)^{-1}\right)^{1/2} \\ &\quad \times \left((-1)^{c_2} a_0^{c_1} x_i \alpha_i\right)^{-1/2} \\ &\equiv \left(c^{-1} H^{-1}\left(H^m(M)\|c^{H(d\|ExpDate)} \bmod n_{\mathrm{RB}}\right)\right) \\ &\quad \times \left((-1)^{c_2} \cdot {a_0}^{-c_1}\right)^{1/2} \\ &\equiv s (\bmod\ n_{\mathrm{RB}}). \end{aligned}$$

Therefore, given a U-token $(d, ExpDate, c_1, c_2, s, c, H(m))$ produced by the scheme, the RB can always derive u and r corresponding to each *view* (α_i, x_i, t_i) such that (2)–(4) are satisfied. In other words, all the U-tokens $(d, ExpDate, c_1, c_2, s, c, H(m))$ are indistinguishable from the RB's point of *view*. Therefore, the RB cannot take advantage of the stored *views* (α_i, x_i, t_i) to link between the MU's identity and a specific signature, which is also defined as the unlinkability or untraceablity property of the blind signature technique. With the unlinkability property, the usage of U-token can provide a strong anonymity to any U-token holders.

3) Unforgeability of U-Token: It will be proven that any attacker cannot forge a new U-token. By the theory of quadratic residues, it is infeasible to compute a square root (or the kth root) of the integer in $Z^*_{n_{\mathrm{RB}}}$ without the factorization of a given quadratic residue integer in $Z^*_{n_{\mathrm{RB}}}$ [34]. Thus, in the proposed U-token issuing protocol, given the integers $\{m, c, d, ExpDate\}$, it is computationally impossible to derive s to form a new U-token without knowing the factorization of n_{RB} such that (1) holds because s is a quadratic residue of the integer $(H(H^m(M)\|c^{H(d\|ExpDate)} \bmod n_{\mathrm{RB}})c)^{-1}$ under the modular n_{RB}.

The proposed scheme is also robust to the chosen-plaintext attack, where an attacker intends to extract a new valid signature by generating a large number of valid partial blind signatures. According to Ferguson's suggestions [38], a blind signature should be injected with one or more randomization factors such that the attacker cannot predict the exact content of the message signed to withstand the chosen-text attack [39], [40]. This is referred to as the randomization property. In the U-token issuing phase, the randomizing factor $c = ux$ is determined by both the signer and the user, and the other users cannot predict or control the generation of c. Hence, the other users cannot replace c with another integer c' because it is intractable to find x from $y = x^{H(d\|ExpDate)} \bmod n_{\mathrm{RB}}$ without knowing the factoring of n_{RB}. Thus, due to the randomization property, even if a user has collected a large number of valid U-tokens, it is impossible for the user to forge a new one.

B. Security Properties of the PPAB Architecture

The proposed PPAB scheme has many attractive security-related properties, which are discussed as follows.

1) Mutual Authentication: A secure roaming scheme should provide a mutual authentication mechanism between the MU and the WISP. In the PPAB architecture, a highly efficient mutual authentication is proposed, where the WISP authenticates itself to the MU by showing its knowledge of the corresponding public/private key pairs, and MU is authenticated based on his authorized credentials, including U-token, subtokens, and $\mathbf{Commit}$. A unique characteristic of the proposed architecture is that an MU can roam across different WISP domains with a single U-token only if this U-token has enough remaining credits.

2) Privacy Preserving: The context privacy of MUs is well protected by the PPAB scheme. According to the privacy definition proposed in Section III-B, PPAB architecture can support privacy preserving from level 1 to level 5. For levels 1 and 2, the communication channel between the MUs and WISP are protected against outsiders by encryption with the shared key PMK. For level 3, due to the unlinkability property of U-tokens, MUs could be authenticated anonymously by the WISPs without disclosing any personal information. For levels 4 and 5, under the cooperation of the RB and the WISPs, using the hash chain could allow the RB and WISPs to link different handoff events in different WISP domains by using the hash values from the same chain to the same user. However, they cannot link different communication sessions to a particular MU due to the underlying unlinkability property of the adopted blind signature techniques. This is regarded as the strongest privacy protection requirement (or intersession unlinkability).

3) Nonrepudiation of Billing: In PPAB, it is promising to achieve nonrepudiated billing of MUs via a lightweight micropayment approach. To pay for the access service, the MU periodically submits his subtokens, which constitute the billing record of this MU. In this approach, a WISP cannot overcharge an MU because it is unable to fake correct subtokens. On the

TABLE I
ABBREVIATIONS OF THE MODULAR OPERATIONS TIME

Notation	Modular Operation Category
T_{MUL}	Time for One modular multiplicative Operation
T_{EXP}	Time for One Modular Exponential Operation
T_{INV}	Time for One Modular Inverse Operation
T_{SQ}	Time for One Modular Square Operation
T_{SQR}	Time for One Modular Square Root Operation
T_{HASH}	Time for One Hash Operation
T_{SE}	Time for One Symmetric Encryption Operation

other hand, the MU cannot deny the bill since no one else can provide correct hash tokens.

VI. EFFICIENCY ANALYSIS

This section analyzes the computation complexity of the proposed architecture. Table I defines the abbreviations of the modular operations in the analysis.

A. Computation Cost

According to [41], the computation time for a modular exponentiation computation is about $O(|n|)$ times of a modular multiplication under modulus n, where $|n|$ denotes the bit length of n, and n is usually taken over 1024 bits to keep a security protocol safe. In addition, an inverse computation in Z_n^* takes almost the same amount of time as that of a modular exponentiation computation in Z_n^* (i.e., $T_{\text{INV}} \approx T_{\text{EXP}}$), and a symmetric encryption operation (or a hashing computation) takes much less time than that of a modular multiplication computation (i.e., $T_{\text{SE}} \approx T_{\text{Hash}} \ll T_{\text{MUL}}$). Since a modular square computation is a special case of modular multiplication computation, we roughly estimate that a modular square computation is equal to a modular multiplication computation, (i.e., $T_{\text{SQ}} \approx T_{\text{MUL}}$), and a modular square root computation can be considered as a modular exponentiation computation (i.e., $T_{\text{SQR}} \approx T_{\text{EXP}}$). Thus, we can have a rough estimation of relationships of various operations. i.e.,

$$T_{\text{INV}} \approx T_{\text{EXP}} \approx T_{\text{SQR}} \approx (O|N|)\, T_{\text{MUL}} \approx (O|N|)\, T_{\text{SQ}} > (O|N|)\, T_{\text{hash}} \approx (O|N|)\, T_{\text{SE}}. \quad (8)$$

In conclusion, modular inversion and exponential and square root operations are three most time-consuming operations among all the cryptographic operations.

The total computation load for the MU is given in Table II. We are only interested in the computation from the user side since the user devices may not have sufficient computation power and may take unacceptably long computation time on those complicated operations.

It is observed that the major power consumption of an MU comes from the blind signature issuing process (i.e., the U-token purchasing and log off phases), where two exponential computations are performed. To reduce the computation in the blind signature process, we can adopt a precomputation technique to speed up the U-token purchasing and log off processes, where d and $ExpDate$ can be determined in advance since they are two public parameters. In addition, several random u can be chosen in advance, and the term $u^{H(d\|ExpDate)}$ can be precomputed and stored in the user's terminal equipment such that the user can make use of them in the purchasing and log off phases. With the precomputation mechanism, Table II can be revised to Table III.

TABLE II
COMPUTATION LOAD FOR MU IN EACH PHASE OF THE PROPOSED ROAMING PROCEDURE

Phase	Computation Cost
U-token Purchase	$2T_{\text{EXP}} + 7T_{\text{MUL}} + 2T_{\text{SQ}} + 2T_{\text{hash}}$
Authenticated Key Agreement	$1T_{\text{SQ}} + 2T_{\text{SE}} + 1T_{\text{hash}}$
Inter domain Handoff	$1T_{\text{SQ}} + 2T_{\text{SE}} + 1T_{\text{HASH}}$

TABLE III
COMPUTATION FOR MU, CONSIDERING THE PRECOMPUTATION MECHANISM

Phase	Computation Cost
U-token Purchasing	$1T_{\text{EXP}} + 7T_{\text{MUL}} + 2T_{\text{SQ}} + 2T_{\text{hash}}$
Authenticated Key Agreement	$1T_{\text{SQ}} + 2T_{\text{SE}} + 1T_{\text{hash}}$
Inter-domain handoff	$1T_{\text{SQ}} + 2T_{\text{SE}} + 1T_{\text{HASH}}$

In terms of the handover process, the corresponding power consumption becomes extremely low by removing the expensive computation effort such as exponential operation during access and roaming procedures. A rough evaluation of computation time and energy consumption is given as follows for a handover process.

B. Seamless Mobility Support

For some real-time applications such as voice services, they have a stringent requirement on delay jitter (i.e., the time variation between two sequential frames) and end-to-end delay (i.e., the time for transmitting a packet from one end to the other). However, the current IEEE 802.1x-based inter-WISP-domain authentication is obviously a very time-consuming process in a handover event that could lead to serious packet drop and delay of real-time service. Therefore, it is crucial to reduce the authentication processing time to keep the real-time application connection and, hence, provide seamless mobility support in WMSNs.

In the proposed PPAB architecture, fast authentication can be achieved as follows.

1) The proposed cryptographic operations required to be performed on-line can be executed with an extremely low latency. Table IV compares the execution time of the proposed handover scheme, RSA-based handover scheme, and ECC-based handover scheme [42]. Since we only take the MU's computation load (particularly the most time-consuming public key operations, including signature verification and encryption operations) into consideration, the computational time for the verification and encryption of public key cryptography (PKC) is of interest. It can be seen that the proposed handover scheme can be executed two times faster than the RSA-based and 30 times faster than the ECC-based handover authentication schemes, respectively.

TABLE IV
LATENCY (IN MILLISECONDS) OF ENCRYPTION AND VERIFICATION OPERATIONS IN VARIOUS PKCs

PKC	Rabin-1024	RSA-1024	ECC-163
Encryption	1.35	2.69	39.22 (ECES)
Verification	1.35	2.69	39.22 (ECDSA)

* Execution time of the Rabin's scheme is estimated from the fact that if the public key is chosen as 3, RSA performs two modular multiplication which yields almost two times of overhead than that by the Rabin's encryption [43]. This fact can also be applied to signature verification.
* Execution time of RSA and ECC encryption and verification comes from [44]. ECC scheme includes Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Encryption Scheme (ECES) [42]

2) The delay can be largely reduced due to the adoption of the proposed localized authentication strategy. In the following sections, we will demonstrate this by evaluating the signaling cost of the PPAB scheme.

We evaluate the handover signaling cost, which is denoted as C_{handover}, of the proposed localized authentication mechanism through an analytical model, where the unit C_{handover} can be defined as *signaling overhead* $*$ *hops* [45]. For each session, the following two types of handovers are defined: 1) inter-WISP handover and 2) intra-WISP handover. Let i be the total number of handover events, j be the number of inter-WISP handover events, and $(i-j)$ be the number of intra-WISP handover events. Then, the total authentication cost due to the handover under the proposed architecture can be expressed as

$$C_{\text{handover}}(i,j) = (i-j) * C_{\text{intra-WISP}} + j * C_{\text{inter-WISP}} \tag{9}$$

where $C_{\text{intra-WISP}}$ and $C_{\text{inter-WISP}}$ are the cost for each intra-WISP handover and inter-WISP handover, respectively. More specifically, $C_{\text{intra-WISP}}$ is determined by the size of authentication message denoted as $Size_{\text{AM}}$ and the average hop counts between AP and the corresponding WISP server D_1, which is denoted as D_1, i.e., $C_{\text{intra-WISP}} = Size_{\text{AM}} * 2 * D_1$. For $C_{\text{inter-WISP}}$, the following two scenarios are defined: 1) with the proposed localized inter-WISP authentication and 2) with nonlocalized inter-WISP authentication. The cost of each localized inter-WISP handover authentication process can be obtained by $C^{\text{local}}_{\text{inter-WISP}} = 2 * Size_{\mathbf{Commit}}$, where $Size_{\mathbf{Commit}}$ is the size of **Commit**. In comparison, each nonlocalized inter-WISP handover authentication cost can be defined as $C^{\text{nonlocal}}_{\text{inter-WISP}} = 2 * Size_{\text{U-token}} * D_2$, where D_2 is the average hop count from the visited AP to the RB, and $Size_{\text{U-token}}$ is the size of the U-token.

To investigate the authentication cost, we follow a widely used analytic model for interdomain and intradomain handovers to compare the proposed localized authentication mechanism with the nonlocalized authentication [46], [49]. Let the residence time of an MU in an AP (or the reciprocal of handover frequency) follow a general distribution with mean $1/(\mu_{\text{AP}})$, whose probability density function (pdf) is $f_{\text{AP}}(t)$ and its Laplace transform is $f^*_{\text{AP}}(t)$. Let the WISP domain residence time of the MU also follow a general distribution with mean $1/(\mu_{\text{WISP}})$, whose pdf is $f_{\text{WISP}}(t)$ and whose Laplace transform is $f^*_{\text{WISP}}(t)$. If the MU arrival time follows an exponential distribution with mean $1/\lambda$, by the handover model [46], the pdfs of i and j can be written as follows:

$$\alpha(i) = \begin{cases} 1 - 1/\rho_{\text{AP}}\left[1 - f^*_{\text{AP}}(\lambda)\right], & \text{if } i = 0 \\ 1/\rho_{\text{AP}}\left[1 - f^*_{\text{AP}}(\lambda)\right]^2 * \left[f^*_{\text{AP}}(\lambda)\right]^{i-1}, & \text{if } i > 0 \end{cases}$$

$$\beta(j) = \begin{cases} 1 - 1/\rho_{\text{WISP}}\left[1 - f^*_{\text{WISP}}(\lambda)\right], & \text{if } j = 0 \\ 1/\rho_{\text{WISP}}\left[1 - f^*_{\text{WISP}}(\lambda)\right]^2 & \\ \quad * \left[f^*_{\text{WISP}}(\lambda)\right]^{j-1}, & \text{if } j > 0 \end{cases}$$

where $\rho_{\text{AP}} = \lambda/\mu_{\text{AP}}$, and $\rho_{\text{WISP}} = \lambda/\mu_{\text{WISP}}$.

Finally, we can calculate the average authentication cost of the proposed localized authentication mechanism as follows:

$$C_{\text{handover}} = \sum_j \sum_i C_{\text{handover}}(i,j) \cdot \alpha(i) \cdot \beta(j). \tag{10}$$

TABLE V
PARAMETERS USED IN NUMERICAL RESULTS (IN BITS)

nounce	t	MU	Receiver	c_1	c_2	Issuer
64	1024	64	64	1	1	64
d	$ExpDate$	c	s	m		
8	64	1024	1024	64		

* Assume all the public key operations are based on $\mathbb{Z}^*_{1024}$ and therefore any intermediate results generated from $\mathbb{Z}^*_{1024}$ such as α, t are 1024 bits

1) Numerical Results: We evaluate the effect of user mobility and the average hop count between each AP and the RB on the authentication signaling cost due to handovers. The data length of parameters related to intra- and inter-WISP handover authentication is given in Table V. Let the number of APs in a WISP domain be 36, D_1 be 2, λ and μ_{AP} be normalized to 1.0, and μ_{WISP} be $\mu_{\text{AP}}/\sqrt{N}$. We first investigate the effect by varying the AP residence time of each MU upon the authentication cost of the MU, where D_2 is set to 2, 5, 8, and 11 for the nonlocalized authentication scheme, respectively. As shown in Fig. 6, the average authentication cost for the proposed localized authentication and the nonlocalized authentication mechanisms are very close to each other when the handover frequency is low. Further, the authentication cost due to the handovers increases as the handover frequency μ_{AP} increases.

When the nonlocalized authentication mechanism is applied, the authentication cost is significantly higher than that of the proposed localized authentication, and the difference becomes larger as the handover frequency increases. The reason is that there exists the large authentication signaling overhead as MUs frequently perform intradomain and interdomain handovers. It is also observed that the average number of hop counts between the visited AP and the RB (D_2) plays an important role in the authentication cost when a nonlocalized authentication method is in place. When the number of hop counts increases, the authentication cost of the nonlocalized authentication method increases as well due to the round-trip signaling propagation by the authentication request/response. On the other hand, the hop counts have little impact on the authentication cost with the proposed localized authentication mechanism. This further demonstrates that achieving localized authentication could be very critical to the overall success of seamless mobility support.

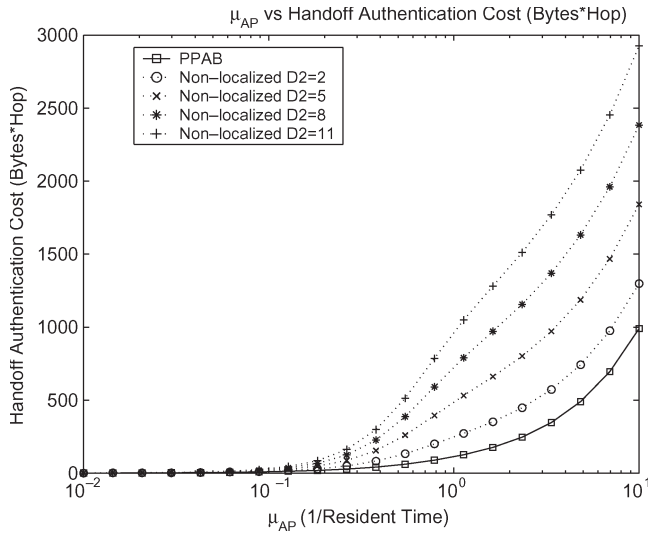


Fig. 6. Average authentication cost due to handovers.

TABLE VI
ENERGY COST OF ENCRYPTION AND SIGNATURE VERIFICATION OF VARIOUS PKCS (IN MILLIJOULES)

Public Key Cryptosystem	Encryption Cost (mJ)	Ciphertext Overhead (bits)	Verification Cost (mJ)	Signature Overhead (bits)
Rabin-1024	7.98	1024	7.98	1024
RSA-1024	15.97	1024	15.97	1024
ECC-163	196.23	320	196.23	320

* The energy cost of digital signature schemes, such as RSA-1024, ECDSA-160 [47].
* The cost of receiving one byte is 28.6 μJ, and the cost of transmitting a byte is 59.2 μJ [48].
* The energy consumption cost for symmetric cipher is extremely low, for example AES is 1.21 $\mu J/Byte$ [47].

C. Energy Efficiency

Energy consumption has become a critical issue in wireless networks, where network nodes are battery-powered devices such as cell phones and laptop computers. Table VI summarizes the energy consumption of various operations involved in the proposed architecture. In addition to Rabin's scheme, the energy cost by RSA and ECC is also listed for comparison.

Let E denote the total energy consumption of a single handover procedure for interdomain roaming. A simple model is used for evaluating the total energy consumption in an inter-WISP handover procedure, which is composed of five components—one verification operation, one asymmetric encryption operation, two symmetric decryption operations, and the transmission and receiving cost. The model is devised such that the energy consumption of various types of encryption and signature schemes for interdomain roaming can be distinguished, i.e.,

$$E_{\text{inter}} = E_{\text{cost}}(V) + E_{\text{cost}}(pe) + E_{\text{cost}}(se) + E_{\text{cost}}(T) + E_{\text{cost}}(R) \quad (11)$$

where V, pe, se, T, and R represent a verification operation, an asymmetric encryption operation, the symmetric decryption operations, the total transmitting operations, and the total receiving operations, respectively.

TABLE VII
ENERGY COST PER INTER-WISP HANDOVER FOR VARIOUS PKCS (IN MILLIJOULES)

	$E_{inter}^{Proposed}$	E_{inter}^{RSA}	E_{inter}^{ECC}
Energy Cost	27.8	43.79	396.07

To compare the proposed handoff authentication scheme, the RSA-based handoff scheme, and the ECC-based handoff scheme, the energy consumption per handoff based on various PKCs are compared and summarized in Table VII, where $E_{\text{cost}}^{\text{Proposed}}$ stands for energy consumption in a handover procedure for the proposed handover authentication architecture, $E_{\text{cost}}^{\text{RSA}}$ stands for energy consumption in a handover procedure for an RSA scheme with 1024 bits, and E_{cost}^{ECC} stands for energy consumption in a handover procedure for an ECC scheme with 163 bits. It can be seen that the proposed scheme has a great advantage in terms of the energy efficiency. The overall energy consumption of the proposed scheme is 38% less of that by RSA and 90% of that by ECC.

The energy consumption of an intra-WISP handover procedure can obtained as follows:

$$E_{\text{intra-WISP}} = E_{\text{cost}}(se) + E_{\text{cost}}(T) + E_{\text{cost}}(R). \quad (12)$$

Let i be the total number of handovers and j be the number of inter-WISP handovers. The total energy consumption taken by authentication can be obtained by

$$E_{\text{handover}}(i,j) = (i-j) * E_{\text{intra-WISP}} + j * E_{\text{inter-WISP}}. \quad (13)$$

The average energy consumption of the proposed localized authentication mechanism based on various PKCs can then be calculated by

$$E_{\text{handover}} = \sum_{j} \sum_{i} E_{\text{handover}}(i,j) \cdot \alpha(i) \cdot \beta(j). \quad (14)$$

1) Numerical Results: We investigate the effect by varying the residence time of an MU in an AP. We assume that, except MUs, all devices in the network, including APs and the RB, are not subject to any power constraint. Thus, we are only interested in investigating the energy consumption due to a handover at an MU while various PKCs are applied.

In Fig. 7, it is observed that the energy consumption of different PKCs is very close to each other when the handover frequency is low. The energy consumption due to the handovers increases as μ_{AP} increases. It is also observed that the energy consumption of the ECC-based scheme increases much more rapidly compared with that by the RSA-based handover authentication scheme and the proposed handover authentication schemes when μ_{AP} increases. The reason is that the verification procedures of the RSA-based scheme and the proposed handover scheme are very efficient compared with that of the ECC-based method.

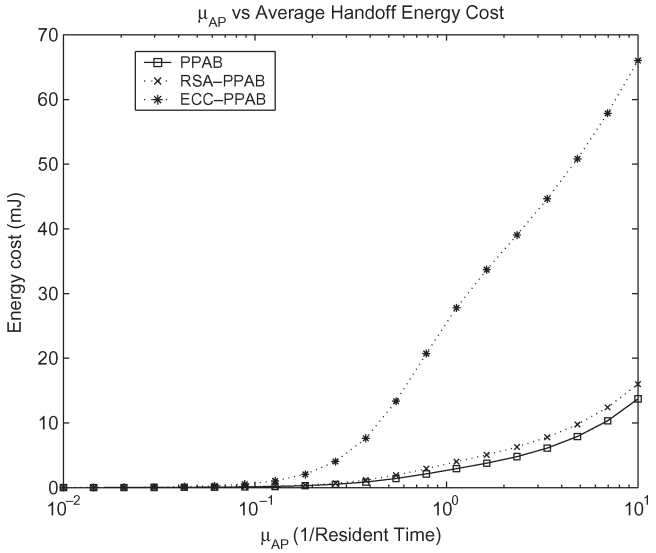


Fig. 7. Average energy cost for inter-WISP handover authentication based on various PKCs.

VII. Conclusion

In this paper, a novel RB-based PPAB architecture has been introduced for the emerging WMSNs composed of numerous WISPs and the associated APs. The proposed architecture not only can avoid the overhead of imposing numerous mutual roaming agreement between each pair of WISPs but can also guarantee the user privacy and identity anonymity. With the proposed partially blind signature mechanism, the required size of the central database at the RB can be significantly reduced. Furthermore, the proposed PPAB architecture is complementary to and can coexist with any other commercialized heterogeneous wireless service billing system with multiple WISPs. In addition, an efficient billing mechanism among MUs, WISPs, and the RB, namely, U-token, has been introduced, aiming at achieving secure and privacy-preserving mutual authentication and billing in a single stage with the presence of frequent interdomain roaming events and a stringent handover delay requirement. We have demonstrated the merits of the proposed PPAB architecture through extensive analysis and discussions. We have also verified the security assurance, computation complexity, and power consumption of the proposed architecture with numerical results and demonstrated that the proposed handover authentication mechanism can significantly outperform the RSA- and ECC-based methods.

References

[1] N. Thompson, G. He, and H. Luo, "Flow scheduling for end-host multihoming," in *Proc. IEEE INFOCOM*, 2006, pp. 1–12.
[2] R. Chakravorty, S. Agarwal, S. Banerjee, and I. Pratt, "MoB: A mobile bazaar for wide-area wireless services," in *Proc. ACM MobiCom*, 2005, pp. 228–242.
[3] E. C. Efstathiou, P. A. Frangoudis, and G. C. Polyzos, "Stimulating participation in wireless community networks," in *Proc. IEEE INFOCOM*, 2006, pp. 1–13.
[4] N. A. Thompson, Z. Yin, H. Luo, P. Zerfos, and J. P. Singh, "Authentication on the edge distributed authentication for a global open Wi-Fi networks," in *Proc. MobiCom*, 2007, pp. 334–337.
[5] M. Bina and G. Gialis, "Emerging issues in researching community-based WLANs," *J. Comput. Inf. Syst.*, vol. 46, no. 1, pp. 9–16, Fall 2005.
[6] G. Ateniese, A. Herzberg, H. Krawczyk, and G. Tsudik, "Untraceable mobility or how to travel incognito," *Comput. Netw.*, vol. 31, no. 8, pp. 871–884, Apr. 1999.
[7] B. Schilit, J. Hong, and M. Gruteser, "Wireless location privacy protection," *Comput.*, vol. 36, no. 12, pp. 135–137, Dec. 2003.
[8] *802.1x*. [Online]. Available: http://standards.ieee.org/getieee802/download/802.1x-2004.pdf
[9] A. Alimian and B. Aboba, "Analysis of roaming techniques," *IEEE. 802.11-04/0377rl*. [Online]. Available: http://www.drizzle.com/~aboba/IEEE
[10] M. Long, C. H. Wu, and J. D. Irwin, "Localised authentication for inter-network roaming across wireless LANs," *Proc. Inst. Elect. Eng.—Commun.*, vol. 151, no. 5, pp. 496–500, Oct. 2004.
[11] Y. Zhang and Y. Fang, "ARSA: An attack-resilient security architecture for multi-hop wireless mesh networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 10, pp. 1916–1928, Oct. 2006.
[12] Y. Zhang and Y. Fang, "A secure authentication and billing architecture for wireless mesh networks," *Wirel. Netw.*, vol. 13, no. 5, pp. 663–678, Oct. 2007.
[13] Z. Cao, H. Zhu, and R. Lu, "Provably secure robust threshold partial blind signature," *Sci. China Ser. E*, vol. 35, no. 12, pp. 1254–1265, 2005.
[14] S. Kim and H. Oh, "An offline check system with reusable refunds," *IEICE Trans. Commun.*, vol. 86, no. 3, pp. 1136–1139, 2003.
[15] H. Zhu, X. Lin, P.-H. Ho, X. Shen, and M. Shi, "TTP based privacy preserving inter-WISP roaming architecture for wireless metropolitan area networks," in *Proc. IEEE WCNC*, Hong Kong, Mar. 2007, pp. 2957–2962.
[16] J. Leu, R. Lai, H. Lin, and W. Shih, "Running cellular/PWLAN services: Practical considerations for cellular/PWLAN architecture supporting interoperator roaming," *IEEE Commun. Mag.*, vol. 44, no. 2, pp. 73–84, Feb. 2006.
[17] *Abitcool Wi-Fi Community*. [Online]. Available: http://www.abitcool.com
[18] *Fon*. [Online]. Available: http://www.fon.com
[19] S. Pack and Y. Choi, "Fast handoff scheme based on mobility prediction in public wireless LAN systems," *Proc. Inst. Elect. Eng.—Commun.*, vol. 151, no. 5, pp. 489–495, Oct. 2004.
[20] A. Mishra, M. H. Shin, N. L. Petroni, J. T. Clancy, and W. A. Arbaugh, "Proactive key distribution using neighbor graphs," *IEEE Wireless Commun.*, vol. 11, no. 1, pp. 26–36, Feb. 2004.
[21] C. Chou and K. G. Shin, "An enhanced inter-access point protocol for uniform intra and intersubnet handovers," *IEEE Trans. Mobile Comput.*, vol. 4, no. 4, pp. 321–334, Jul./Aug. 2005.
[22] H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "SLAB: Secure localized authentication and billing scheme for wireless mesh networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 10, pp. 3858–3868, Oct. 2008.
[23] M. Shi, H. Rutagemwa, X. Shen, J. W. Mark, and A. Saleh, "A service-agent-based roaming architecture for WLAN/cellular integrated networks," *IEEE Trans. Veh. Technol.*, vol. 56, no. 5, pp. 3168–3181, Sep. 2007.
[24] M. Shi, L. Xu, X. Shen, and J. W. Mark, "Fast vertical handoff for cellular and WLAN interworking," *Wiley's Wireless Commun. Mobile Comput.*, vol. 7, no. 5, pp. 581–594, 2007.
[25] N. Ben Salem, J.-P. Hubaux, and M. Jakobsson, "Fuelling WiFi deployment: A reputation-based solution," in *Proc. WiOpt*, 2004.
[26] E. C. Efstathiou and G. C. Polyzos, "Self-organisation in mobile networking," *Eur. Trans. Telecommun.*, vol. 16, pp. 471–482, 2005.
[27] Y. Tsiounis, A. Kiayias, and A. Karygiannis, "A solution for wireless privacy and payments based on E-cash," in *Proc. IEEE SecureComm*, Athens, Greece, Sep. 2005, pp. 206–218.
[28] B. Askwith, M. Merabti, and Q. Shi, "MNPA: A mobile network privacy architecture," *Comput. Commun.*, vol. 23, no. 18, pp. 1777–1788, Dec. 2000.
[29] S. Choi and K. Kim, "Authentication and payment protocol preserving location privacy in mobile IP," in *Proc. IEEE GLOBECOM*, San Francisco, CA, 2003, vol. 3, pp. 1410–1414.
[30] Q. He, D. Wu, and P. Khosla, "The quest for personal control over mobile location privacy," *IEEE Commun. Mag.*, vol. 42, no. 5, pp. 130–136, May 2004.
[31] M. Stadler, J. M. Piveteau, and J. Camenisch, "Fair blind signatures," in *Proc. Eurocrypt*, 1995, vol. 921, pp. 209–219.
[32] D. Chaum, "Blind signatures for untraceable payments," in *Proc. CRYPTO*. New York: Springer-Verlag, vol. 1982, pp. 199–203.
[33] M. Abe and E. Fujisaki, "How to date blind signatures," in *Proc. ASIACRYPT*. New York: Springer-Verlag, 1996, vol. 1163, pp. 244–251.
[34] M. O. Rabin, "Digitized signatures and public-key functions as intractable as factorization," Mass. Inst. Technol. Lab. Comput. Sci, Cambridge, MA, Tech. Rep. LCS/TR-212, 1979.

[35] S. Seys and B. Prenee, "Efficient cooperative signature: A novel authentication scheme for sensor networks," in *Proc. SPC*. New York: Spring-Verlag, 2005, vol. 3450, pp. 86–100.
[36] T. P. Pedersen, "Electronic payments of small amounts," in *Proc. Cambridge Workshop Security Protocols*, 1996, vol. 1189, pp. 59–68.
[37] I. Osipkov, E. Y. Vasserman, and N. Hopper, "Combating double-spending using cooperative P2P systems," in *Proc. ICDCS*, 2007, p. 41.
[38] N. Ferguson, "Single term off-line coins," in *Proc. EUROCRYPT*. New York: Springer-Verlag, 1993, vol. 765, pp. 318–328.
[39] Y. Desmedt and A. Odlyzko, "A chosen text attack on the RSA cryptosystem and some discrete logarithm schemes," in *Proc. CRYPTO*. New York: Springer-Verlag, 1985, vol. 218, pp. 516–552.
[40] J. S. Coron, D. Naccache, and J. P. Stern, "On the security of RSA padding," in *Proc. CRYPTO*. New York: Springer-Verlag, 1999, vol. 1666, pp. 1–18.
[41] G. J. Simmons, *Contemporary Cryptology: The Science of Information Integrity*. New York: IEEE Press, 1992.
[42] IEEE Working Group P1363, *Working Draft: Standard for RSA, Diffie-Hellman and Related Public-Key Cryptography*, Mar. 1997.
[43] C. K. Wong and S. S. Lam, "Digital signatures for flows and multicasts," *IEEE/ACM Trans. Netw.*, vol. 7, no. 4, pp. 502–513, Aug. 1999.
[44] P. Prasithsangaree and P. Krishnamurthy, "A variation of the WTLS authentication protocol for reducing energy consumption in wireless devices," in *Proc. 7th IEEE Int. Conf. High Speed Netw. Multimedia Commun.*, Toulouse, France, 2004, pp. 696–706.
[45] S. Lo, G. Lee, W. Chen, and J. Liu, "Architecture for mobility and QoS support in all-IP wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 22, no. 4, pp. 691–705, May 2004.
[46] Y. Lin, "Reducing location update cost in a PCS network," *IEEE/ACM Trans. Netw.*, vol. 5, no. 2, pp. 25–33, Feb. 1997.
[47] N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," *IEEE Trans. Mobile Comput.*, vol. 5, no. 2, pp. 128–143, Mar./Apr. 2006.
[48] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in *Proc. IEEE PerCom*, Pisa, Italy, Mar. 2005, pp. 324–328.
[49] S. Baek, S. Pack, T. Kwon, and Y. Choi, "A localized authentication, authorization, and accounting (AAA) protocol for mobile hotspots," in *Proc. 3rd Annu. Conf. Wireless On-Demand Netw. Syst. Serv., WONS*, 2006, pp. 144–153.

Haojin Zhu received the B.Sc. degree from Wuhan University, Wuhan, China, in 2002 and the M.Sc. degree from Shanghai Jiao Tong University, Shanghai, China, in 2005, both in computer science. He is currently working toward the Ph.D. degree in electrical and computer engineering with the Center for Wireless Communications, Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada.

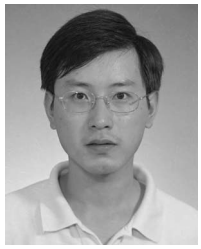
His current research interests include wireless network security and applied cryptography.

Mr. Zhu was the recipient of Best Paper Awards at the 2007 IEEE International Communications Conference: Computer and Communications Security Symposium, and at the 2008 Third International Conference on Communications and Networking in China: Wireless Communication Symposium.

Xiaodong Lin received the Ph.D. degree in information engineering from Beijing University of Posts and Telecommunications, Beijing, China, in June 1998 and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in June 2008.

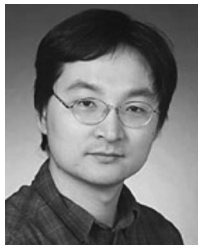
He is currently an Assistant Professor with the Faculty of Business and Information Technology, Institute of Technology, University of Ontario, Oshawa, ON. His research interests include wireless network security, applied cryptography, and anomaly-based intrusion detection.

Dr. Lin received the Natural Sciences and Engineering Research Council of Canada Canada Graduate Scholarships (CGS) Doctoral and Best Paper Awards at the 2007 IEEE International Communications Conference: Computer and Communications Security Symposium, and the 2008 Third International Conference on Communications and Networking in China: Wireless Communication Symposium.



Minghui Shi received the B.S. degree from Shanghai Jiao Tong University, Shanghai, China, in 1996 and the M.S. and Ph.D. degrees from the University of Waterloo, Waterloo, ON, Canada, in 2002 and 2006, respectively, all in electrical engineering.

He was a Natural Sciences and Engineering Research Council of Canada Postdoctoral Fellow with McMaster University, Hamilton, ON, from 2006 to 2008. He is currently a Visiting Scientist with the Center for Wireless Communications, Department of Electrical and Computer Engineering, University of Waterloo. His current research interests include security protocol and architecture design, authentication and key distribution for ad hoc/sensor networks, heterogeneous network interworking, delay-tolerant networks, and vehicular networks.



Pin-Han Ho (M'04) received the B.Sc. and M.Sc. degrees from the National Taiwan University, Taipei, Taiwan, in 1993 and 1995, respectively, and the Ph.D. degree from the University of Waterloo, Waterloo, ON, Canada, in 2002.

In 2003, he joined the Department of Electrical and Computer Engineering (ECE), University of Waterloo, where he is currently an Associate Professor with the Center for Wireless Communications. He is the author or a coauthor of more than 100 refereed technical papers and book chapters and a coauthor of a book on optical networking and survivability.

Mr. Ho is the recipient of the Distinguished Research Excellent Award from the Department of ECE, University of Waterloo, the Early Researcher Award (Premier Research Excellence Award), the Best Paper Award at the 2002 International Symposium on Performance Evaluation of Computer and Telecommunication Systems and the 2005 and 2007 IEEE International Communications Conference, and the Outstanding Paper Award at the 2002 IEEE High-Speed Switching and Routing Conference.

Xuemin (Sherman) Shen (M'97–SM'02–F'09) received the B.Sc. degree from Dalian Maritime University, Dalian, China, in 1982 and the M.Sc. and Ph.D. degrees from Rutgers University, Camden, NJ, in 1987 and 1990, respectively, all in electrical engineering.

He is a Professor and a University Research Chair and the Associate Chair for Graduate Studies with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. He serves as the Editor-in-Chief for *Peer-to-Peer Networking and Application* and as an Associate Editor for *Computer Networks*, *ACM/Wireless Networks*, and *Wireless Communications and Mobile Computing*. His research focuses on mobility and resource management in interconnected wireless/wireline networks, ultra-wideband wireless communications systems, wireless security, and ad hoc and sensor networks. He is a coauthor of three books and has published more than 300 papers and book chapters in wireless communications and networks, control, and filtering.

Dr. Shen is a Registered Professional Engineer in the Province of Ontario. He served as the Technical Program Committee Chair of the 2007 IEEE Global Communications Conference, a General Cochair of the 2007 International Conference on Communications and Networking in China and the 2006 Third International Conference on Heterogeneous Networking for Quality, Reliability, Security, and Robustness, and the Founding Chair of the IEEE Communications Society Technical Committee on P2P Communications and Networking. He also serves as a Founding Area Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and as an Associate Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and the KICS/IEEE JOURNAL OF COMMUNICATIONS AND NETWORKS. He has also served as a Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, *IEEE Wireless Communications*, and the *IEEE Communications Magazine*. He received the Excellent Graduate Supervision Award and the Outstanding Performance Award from the University of Waterloo in 2006 and 2004, respectively, the Premier's Research Excellence Award from the Province of Ontario in 2003, and the Distinguished Performance Award from the Faculty of Engineering, University of Waterloo, in 2002.