SLAB: A Secure Localized Authentication and Billing Scheme for Wireless Mesh Networks

Haojin Zhu, Xiaodong Lin, *Student Member, IEEE,* Rongxing Lu, Pin-Han Ho, *Member, IEEE,* and Xuemin (Sherman) Shen, *Senior Member, IEEE*

***Abstract*—The future metropolitan-area wireless mesh networks (WMNs) are expected to contain compromise-prone Mesh Access Points (MAPs) with a high frequency of inter-domain roaming/handoff events. This paper introduces a novel secure localized authentication and billing (SLAB) scheme, which aims to address both security guarantee and performance in terms of system compromise resilience capability, inter-domain handoff authentication latency, and workload of the roaming broker (RB). With extensive analysis and simulation, we demonstrate that the proposed scheme can be a practical solution for achieving secure roaming and billing in metropolitan-area WMNs.**

***Index Terms*—Wireless mesh networks, security, inter-domain handoff, authentication and billing.**

I. Introduction

WIRELESS mesh networks (WMNs) have been demonstrated having a great potential to reshape the communications landscape by forming a burgeoning market for the next-generation Internet services in the foreseeable future [1]. The metropolitan-area WMNs are expected to accommodate numerous network domains, which are mainly composed of a number of physically adjacent Mesh Access Points (MAPs) as Extended Service Set (ESS) and a mesh gateway (MGW) as the interfaces to connect the ESS with the public Internet. These different WISP domains can be operated by independent Wireless Internet Service Providers (WISPs). A mobile user can enjoy pervasive Internet services in presence of high mobility by roaming among these different WISP domains. However, the security concerns in WMNs still remain a serious impediment to widespread adoption of the considered application scenario.

The current widely accepted security solution for WMNs is based on Authentication, Authorization and Accounting (AAA) architecture [2], where the authentication request is issued by the mobile user (MU) and is sent through the serving MAP (sMAP) and the MGW, until reaching a centralized authentication server (such as RADIUS) that can grant access to the MU [3]. Such a long signaling path, however, could take up to one or a few seconds of propagation, and might cause fatal impairment on the emerging real-time services. Recently, many fast authentication schemes such as predictive authentication [4], pre-key-distributions [5], and enhanced inter-access point protocol (IAPP) [6], have been reported to support seamless handover when an MU roams between adjacent MAPs under a common WISP domain (also referred to as intra-domain handoff). On the other hand, the existing fast authentication techniques cannot be directly applied to inter-domain handoff, since it requires a bilateral service level agreement (SLA) established between each pair of WISPs. Such a peer-to-peer approach may lead to a scalability problem in the presence of numerous WISPs in the WMN [7].

The best practice for establishing a trust relationship among different WISPs so far is by way of a centralized roaming broker (RB) trusted by all the WISPs [8]. Under this framework, when an MU roams into a foreign network domain, the foreign WISP simply forwards the corresponding AAA session of the MU to the home WISP of the MU for authorization via the RB. A more elaborated approach can be devised on top of the centralized RB architecture by taking advantages of the public key infrastructure (PKI), where the RB serves as not only a trusted third party, but also a certificate authority (CA) which issues public key certificates to the WISPs and MUs. The trust relationship among WISPs, or between a WISP and MUs, can be easily established by validating the public key certificates issued by the RB [7], [9]. In both cases, the foreign WISP reports the accounting information of the roaming MU to its home WISP at the completion of the session, by which the home WISP will pay the bill and then charge the MU in terms of the MU's spending. The RB architecture can effectively solve the inter-domain roaming and billing problem; unfortunately, the RB may become a performance bottleneck for the inter-domain handoff authentication and billing. In addition, the long signaling propagation latency of every transaction may not be tolerable to the real-time services in the inter-domain roaming events. Thus, it is desirable to develop a new framework in meeting with the stringent requirements on authentication latency and scalability without losing the security assurance.

To achieve scalable, secure and efficient authentication and billing, the following two observations are made:

- Firstly, since each WISP not only serves as a vendor providing services to the MUs, but also a buyer, which purchases services from other WISPs for the MUs, the multi-WISP WMNs can be taken as both a business-to-business (B2B) system (WISP - WISP) and a business-

Manuscript received April 20, 2007; revised September 6, 2007; accepted September 30, 2007. The associate editor coordinating the review of this paper and approving it for publication was Y. Fang. This work was supported by research grants from Provincial Centre of Excellence Communications and Information Technology Ontario (CITO), Canada.

The authors are with the Centre for Wireless Communications, Department of Electrical and Computer Engineering, University of Waterloo, 200 University Avenue West, Waterloo, Ontario, Canada N2L 3G1 (e-mail: {h9zhu, xdlin, rxlu, pinhan, xshen}@bbcr.uwaterloo.ca).

Digital Object Identifier 10.1109/T-WC.2008.07418

to-consumer (B2C) system (WISP - MU). Therefore, from the WISPs' point of view, an inter-domain handoff can be taken as an inter-WISP payment; while from the MUs' point of view, an MU can roam into another WISP domain if and only if he has enough remaining credits. Thus, a WISP can issue a digital signature based on PKI, which serves as the digital currency for electronically performing inter-domain payment with another WISP without intervention of the RB. In addition, this digital signature can also be taken as an authentication credential of the corresponding MU, which is authenticated every time when the MU requests for inter-domain roaming. In this paper, we define such a digital signature as "*D-coin*".

- Secondly, by pre-loading each MAP with necessary cryptographic information, some required security capability can be achieved such that the roaming/handoff authentication and billing can be performed in a localized manner with much better scalability. Such a localized authentication and billing scheme is expected to effectively solve the scalability problem due to the centralized RB and dramatically reduce the inter-domain roaming latency by avoiding any intervention of the RB.

The advantages gained in localizing the authentication and billing, however, are at the expense of reduced security level of the system due to the compromise-prone MAPs which are most likely low-cost devices without expensive and wholesome protection [10]. In a compromise event, the cryptographic secrets, such as the public/secret key pairs, could be deprived by the attackers, who may launch some serious attacks by manipulating the secret information. For example, the attacker can manipulate a compromised MAP to arbitrarily issue D-coin to an illegal MU or accept D-coin without granting services to the MU (or referred to as the *Coin Fraud attack*), or overcharge an MU by holding the connection even when the MU has disconnected from the MAP (or referred to as the *Overcharge attack*).

In this paper, we propose a novel **S**ecure **L**ocalized **A**uthentication and **B**illing scheme, called SLAB, by manipulating the D-coin. To thwart various attacks due to compromised MAPs, we adopt a *local voting strategy* and the threshold digital signature mechanism to enhance the overall security assurance [11]. With the local voting strategy, the D-coin is issued under the endorsement of not only the serving MAP (sMAP), but also its neighboring MAPs (nMAPs), instead of by any single MAP. To perform billing on-line during the user authentication phase, a local user accounting profile (LUAP), which records each accessing and roaming MU's spending information, is defined and maintained at both sMAP and nMAPs. With SLAB, an inter-domain handoff authentication and billing can be performed in a peer-to-peer manner, where no intervention of the RB is required when an MU roams from its sMAP to the target MAP (tMAP) that belongs to a different WISP. The RB, on the other hand, only needs to be involved during the clearance phase that can be performed off-line, in which a WISP submits its collected D-coin issued by the other WISPs to the RB for payment. To further reduce the workload of the RB in the clearance phase, we take advantages of the short and aggregate digital signature technique [12] to effectively reduce the computational and storage costs on the RB due to the D-coin verification and storage.

The remainder of the paper is organized as follows. Section II reviews the related work along with some preliminary background. In Section III, the proposed SLAB scheme is presented in detail. Section IV analyzes the security of SLAB. Performance analysis is given in Section V, followed by comprehensive discussions on the superiority of the proposed scheme in Section VI. Finally, Section VII concludes the paper.

II. Related Work and Background

A. Related Work

Most previously reported studies on roaming, billing and authentication across multiple logical WISP domains have focused on how to reduce inter-domain handover authentication delay. In [13], [14], it is suggested to make use of a local AAA server 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 seamless inter-domain handover for those roaming MUs which did not visit the wireless domain before. In [7], [9], [15], the PKI is used to build the trust relationship among RB, WISPs and MUs. Based on public key certificates, which can be verified by any network entity anytime, an efficient localized authentication scheme was introduced for inter-WISP roaming across wireless LANs. However, the issues on the inter-WISP billing were not considered as a whole. By envisioning that the future WMAN applications and services could be provisioned in a very dynamic and adaptive fashion, the billing issues must be considered at the same time so as to protect both the WISPs and customers. In [16], based on PKI, we introduced the digital signature based inter-domain roaming and billing architecture, where a WISP not only accepts a valid public key certificate owned by another WISP but also accepts the digital signature issued by that WISP as a payment technique. Therefore, the inter-domain authentication and billing are performed simultaneously by validating a digital signature. However, it is assumed in [16] that every access point is trustable enough to issue the digital signature on behalf of the WISP, which may not be acceptable in WMNs with compromise-prone MAPs. Furthermore, it does not take the workload of RB into consideration, which may easily form a performance bottleneck in an inter-domain handoff scheme.

B. Short Digital Signature and Aggregate Signature

The proposed SLAB scheme is based on a short and aggregate digital signature technique. The short digital signature technique has been taken as an effective approach in the classic cryptographic research area for reducing digital signature overhead. A number of short signature schemes have been reported in the literature. Boneh made use of weil pairing to build the shortest digital signature [12]. Compared with RSA signature sized 1024 bits and ECDSA signature sized

320 bits, a short digital signature is only 160 bits in length. In the wireless communication scenario, adopting a signature with an extremely small size can save the precious wireless communication resources and transmission power at the MUs. Furthermore, in case multiple pieces of D-coin is submitted to the RB for verification and clearance, it is desirable to aggregate the multiple pieces of D-coin into a single piece of D-coin by applying the aggregate signature technique [12] in order to save both transmission and computation costs. The short and aggregate signature can be achieved by bilinear pairing, which is briefly introduced as below.

Let $\mathbb{G}_1$, $\mathbb{G}_1'$ be two cyclic additive groups and $\mathbb{G}_2$ be a cyclic multiplicative group of the same prime order q, i.e., $|\mathbb{G}_1| = |\mathbb{G}_1'| = |\mathbb{G}_2| = q$. Let P be a generator of $\mathbb{G}_1$, P' be a generator of $\mathbb{G}_1'$, and ψ be an isomorphism from $\mathbb{G}_1'$ to $\mathbb{G}_1$, with $\psi(P') = P$. An admissible bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1' \rightarrow \mathbb{G}_2$ satisfies the following properties:

- Bilinear: for all $P_1 \in \mathbb{G}_1$, $Q_1 \in \mathbb{G}_1'$ and $a, b \in \mathbb{Z}_q^*$, $\hat{e}(aP_1, bQ_1) = \hat{e}(P_1, Q_1)^{ab}$.
- Non-degenerate: there exist $P_1 \in \mathbb{G}_1$ and $Q_1 \in \mathbb{G}_1'$ such that $\hat{e}(P_1, Q_1) \neq 1$.
- Computable: there is an efficient algorithm to compute $\hat{e}(P_1, Q_1)$ for any $P_1 \in \mathbb{G}_1$, $Q_1 \in \mathbb{G}_1'$.

Such an admissible bilinear map $\hat{e}$ can be constructed by Weil or Tate pairings on the elliptic curves. According to [17], by software and hardware acceleration, pairing operations can be efficiently accomplished within 1.3 ms.

III. The Proposed SLAB Scheme

A. Trust Relationship Establishment and Security assumptions

The proposed SLAB scheme can be roughly categorized into five major components: (1) Signing key distribution Phase; (2) Secure session maintenance and LUAP generation phase; (3) Localized LUAP transfer during intra-domain handoff phase; (4) D-coin issuing and inter-domain handoff authentication phase; and (5) Clearance phase. Only phase (4) is performed on-line in an inter-domain handoff event, while the others are conducted off-line for the maintenance or preparation of the future handoff events.

SLAB is based on the traditional PKI architecture to build the trust relationship among different WISPs, and between WISPs and MUs by way of the RB. Similar to [16], the RB can serve as a certificate authority (CA) and issue every legitimate WISP with its corresponding certificate such that each WISP can check the validity of another. We assume that a legitimate WISP does not intentionally misbehave, which is reasonable since the attacks on its MUs will decrease the satisfactory of MUs on the WISP, and will lead to reduction of its long-term revenue. On the other hand, the attacks launched by a WISP can be easily detected by the RB, and the malicious WISP will be deprived of its WISP qualification with subsequent penalties. Furthermore, since the number of revoked WISPs should be small for most of the time, it is feasible to real-time update and distribute the certificate revocation list (CRL) of WISPs. The trust relationship also exists between MUs and WISPs, where an MU can check the validity of a WISP by verifying the WISP's certificate issued by the RB.

We also assume that a hierarchical public key system is established in every WISP domain, which includes a domain public/private key preloaded at the MGW along with a number of MAP level public/private keys corresponding to every MAP. Since the MGW is difficult to be compromised, it can thus be fully trusted to serve as the security administrator in any WMN domain. However, since proposed SLAB is a localized and distributed security scheme, MGW gets involved only during the key distribution phase or when some attacks or disputes take place. For simplicity, the communication among MAPs within a common WISP can be transmitted in a secure channel since it is easy for different MAPs to make an authenticated key agreement with their corresponding public/private key. In this paper, we focus on the authentication and billing related attacks.

B. Signing Key Distribution

To jointly issue a piece of D-coin on behalf of the MGW, each MAP will have to obtain a partition of the signing key and implement the threshold digital signature technique. This is considered as the most effective approach to improve the compromise resilience of the WMNs and mitigate the side effect in localizing the D-coin operation.

1) System Parameters and Initialization: The SLAB scheme adopts similar bilinear pairing system parameters $(q^A, \mathbb{G}_1^A, \mathbb{G}_1'^A, \mathbb{G}_2^A, \hat{e}^A, P^A)$ as in [12], where A refers to the name of the currently serving WISP of the MU. WISP A can generate its system parameters, and then choose a random number $s^A \in Z_{q^A}^*$ as its private key which corresponds to the public key expressed as $Y^A = s^A P^A$. In addition, two hash functions are formed: $H : \{0,1\}^* \rightarrow \{0,1\}^l$ and $H_2 : \{0,1\}^* \rightarrow G_1^A$, where l is a pre-defined security parameter. The public key and system parameters $(q^A, \mathbb{G}_1^A, \mathbb{G}_1'^A, \mathbb{G}_2^A, \hat{e}^A, P^A, Y^A, H, H_2)$ along with a public key certificate issued by the trusted RB will be periodically broadcasted to each MU and MAP within the WISP A domain.

2) Signing Key Distribution Phase: The signing key distribution phase can be described as follows. Let $\overline{P^A}$ be a generator of G_1^A such that $\overline{P^A} = \alpha P^A$ for some $\alpha \in Z_{q^A}^*$ while it is infeasible to derive α given P^A and $\overline{P^A}$. To enable the receivers to verify the received signing keys and prevent the active adversaries from injecting invalid ones, the MGW randomly picks up two polynomials $f(x) = s + a_1 x + \cdots + a_{k-1} x^{k-1}$ and $f'(x) = b_0 + b_1 x + \cdots + b_{k-1} x^{k-1}$ of degree $k-1$ such that $f(0) = a_0 = s$ and $f'(0) = b_0$. Then, MGW computes and broadcasts $C_i = a_i P^A + b_i \overline{P^A}$ for $i = 0, 1, \cdots, k-1$ to all the MAPs. Further, MGW computes $f(j)$ and $f'(j)$ secretly and sends them to MAP_j, where $j = 1, \cdots, n$. Any MAP_j can verify the received share by checking whether $f(j)P^A + f'(j)\overline{P^A} = \sum_{i=0}^{k-1} j^i \times C_i$ holds. If the verification holds, $s_j = f(j)$ will be stored by MAP_j as its secret share.

C. Secure Session Maintenance and LUAP Generation Phase

With SLAB, the sMAP of an MU has to collaboratively generate and maintain the local user accounting profile (LUAP) of the MU with some of the nMAPs in order to timely reflect

the spending information of the MU. However, updating the LUAP relies on a secure accounting protocol; otherwise, a compromised MAP may arbitrarily change the accounting information of an MU. Therefore, to achieve incontestable payment and authenticity, the idea of micro-payment [18] is exercised to maintain a secure communication session and the LUAP, by which the MUs are forced to periodically submit a non-repudiation proof of the previous spending information to maintain the session consistency.

Every MU has a predefined maximum consuming credit $\mathcal{B}$. If the MU is gaining access with its home WISP, this balance is the remaining credit in its account. If the MU is gaining access with a foreign WISP using D-coin, $\mathcal{B}$ is taken as the face value defined in the D-coin. Based on $\mathcal{B}$, an MU selects a random integer M and computes a one-way hash chain $H^m(M) = H(H(\cdots(H(M)\cdots)))$ by applying the one-way function $H()$ to M for m times, where every hash token $H^i(M), i \in [1, \cdots, m]$ stands for a monetary value τ such that $\mathcal{B} = m \times \tau$. In the beginning, the MU sends $H^m(M)$ to the MGW in a full IEEE 802.1X authentication scheme or by embedding $H^m(M)$ in the D-coin, which will be further discussed in Section III-E. Thus, MGW can distribute $H^m(M)$ to the nMAPs and sMAP with neighbor graphs technique introduced in [19]. The sMAP and nMAPs will initialize a local user accounting profile for this new user and stores $H^m(M)$ as the commitment. The initial LUAP can therefore be defined as $(ID_{MU}, \mathcal{B}, H^m(M), PMK)$. Here, PMK refers to the pairwise master key (PMK) between the MU and sMAP. According to IEEE 802.11i standard, PMK can be used to derive various transient keys (PTKs) for link layer encryption or data authenticity [20]. It is important to point out that, since SLAB requires pre-storing PMK at nMAPs, any existing pre-key-distribution techniques such as [5], [19] can be employed to realize the fast intra-domain handoff.

When the amount of spending of the MU equals τ money units, it triggers the submission of the first spending proof $SP_1 = H^{m-1}(M)$, which is sent by the MU to its sMAP. To ensure that the LUAPs stored at the sMAP and its one-hop neighbors have also been updated correctly, a receiving acknowledgement from both of the sMAP and nMPAs will be sent to the MGW. Firstly, the sMAP can check the validity of this proof by simply verifying if $H(SP_1) = H^m(M)$ holds. If valid, the SP_1 will be forwarded to the nMAPs. If the verification passes, the $i-th$ nMAP will send back the receiving acknowledgement $AK^1_{nMAP_i} = H(SP_1||K_{nMAP_i,MGW})$ to sMAP, where $K_{nMAP_i,MGW}$ refers to the shared key between $nMAP_i$ and MGW. After receiving the acknowledgements $AK^i_{nMAP_i}, i \in \{1, \cdots, \mathcal{N}\}$ from its $\mathcal{N}$ one-hop neighbors, the sMAP can also compute its acknowledgement $AK^1_{sMAP} = H(SP_1||K_{sMAP,MGW})$ and the aggregate acknowledgement $AK^1 = H(AK^1_{sMAP}||AK^1_{nMAP_1}||\cdots||AK^1_{nMAP_\mathcal{N}})$. Then, the first spending proof as well as the LUAP updating acknowledgement (SP_1, AK^1) is submitted to MGW. Meanwhile, sMAP and nMAPs update their stored LUAP to $(ID_{MU}, \mathcal{B}-\tau, SP_1, PMK)$. After receiving (SP_1, AK^1), MGW can check its validity by checking if the following two conditions hold

1) $H(SP_1) = H^m(M)$.
2) $AK^1 = H(AK^1_{sMAP}||AK^1_{nMAP_1}||\cdots||AK^1_{nMAP_\mathcal{N}})$.

If these two conditions hold, the MGW will accept SP_1 as the first spending proof of the MU, and the LUAPs stored at the sMAP and nMAPs can be updated to $(ID_{MU}, \mathcal{B}-\tau, SP_1, PMK)$. In this way, the MU could reveal $SP_2 = H^{m-2}(M), \cdots, SP_i = H^{m-i}(M), \cdots, SP_m = H^0(M) = M$ one after another to prove the spending for m times. Correspondingly, the LUAPs at the sMAP and nMAPs can be updated to $(ID_{MU}, \mathcal{B}-2\tau, SP_2, PMK), \cdots, (ID_{MU}, \mathcal{B}-i\times\tau, SP_i, PMK), \cdots, (ID_{MU}, \mathcal{B}-m\times\tau = 0, SP_m, PMK)$. In case the hash chain runs out or the MU cannot submit a valid chain token on time, the MGW can detect it and terminate this communication session immediately.

D. Localized LUAP Transfer during Intra-Domain Handoff Phase

An intra-domain handoff means an active communication session changes its network attachment point from the serving MAP to the target MAP within a common WISP domain. The intra-domain handoff will result in a switch of the sMAP and the corresponding set of nMAPs. Thus, the LUAP transfer is performed to ensure that every new nMAP of this MU can obtain a copy of the MU's authentic LUAP. To reduce the multi-hop signaling, we propose a localized LUAP transfer algorithm based on localized voting strategy which is defined as that the LUAP can be accepted as a valid one if and only if there are more than k valid LUAP copies from the nMAPs being consistent. Let $Neighbor(MAP_i)$ denote the set of nMAPs of MAP_i, $Local(MAP_i) = Neighbor(MAP_i) \bigcup MAP_i$ denote the nMAPs and itself, $LUAP(MU)$ denote the LUAP of the MU, and $Cache(MAP_i)$ denote the caches maintained at MAP_i. Let $Obtain\_LUAP(MAP_{Source}, MU, MAP_{Destination})$ be the function invoked by $MAP_{Destination}$ for obtaining a LUAP copy of an MU. Let $Check\_LUAP(MAP_i, MU)$ be the function invoked by MAP_i for checking the LUAPs in hand and decide if they are consistent. This function will return the maximum number of consistent LUAPs. Let $Insert\_Cache(MAP_i, LUAP(MU))$ and $Remove\_Cache(MAP_i, LUAP(MU))$ be the functions that insert and remove the LUAP of the MU to and from the cache of MAP_i, respectively. The LUAP transfer algorithm is presented in Algorithm 1.

Suppose that an MU is currently associated to MAP_G and he is going to handoff to MAP_H, as shown in Fig.1. In this process, the sMAP and nMAP set of the MU will switch from $Local(G) = \{D, E, G, H\}$ to $Local(H) = \{D, E, F, G, H, I\}$. Therefore, two new nMAPs $\{F, I\}$ need to obtain the LUAP of MU from $Local(G)$. $\{F, I\}$ can contact any MAPs in $Local(G)$ to obtain their stored $LUAP(MU)$. If more than k LUAPs among the obtained $LUAP(MU)$ are consistent, $\{F, I\}$ will store the consistent LUAP in its caches. Otherwise, it will return a fault alert to the MGW. Because the LUAP transfer algorithm can be proceeded in a peer-to-peer fashion among MAPs without intervention of the MGW, the LUAP transfer can be performed in a localized manner.

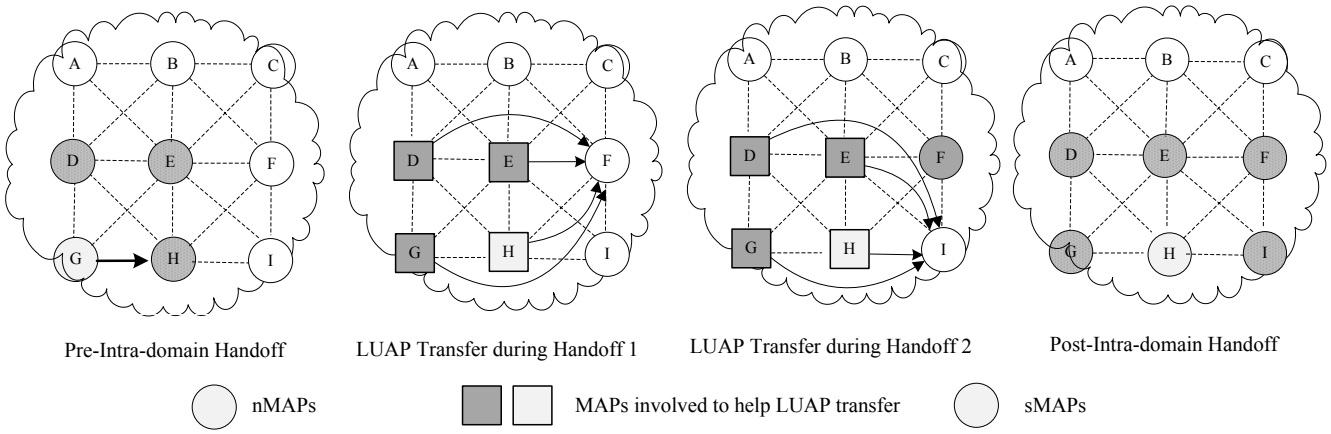


Fig. 1. LUAP transfer during intra-domain handoff

Algorithm 1: Localized LUAP Transfer

Data: $(sMAP, MU, tMAP)$
Result: `valid` or `invalid`
begin
  for $MAP_i \in Neighbor(tMAP) \wedge LUAP(MU) \notin cache(MAP_i)$ **do**
    for $MAP_j \in Local(sMAP)$ **do**
      $Obtain\_LUAP(MAP_j, MU, MAP_i)$
    end
    if $Check\_LUAP(MAP_i, MU) \geq k$ **then**
      $Insert\_Cache(MAP_i, LUAP(MU))$
    else
      return `invalid`
    end
  end
  for $MAP_i \in Neighbor(sMAP) \wedge \notin Local(tMAP)$ **do**
    $Remove\_Cache(MAP_i, LUAP(MU))$
  end
  return `valid`
end

The most expensive operation in Algorithm 1 is the method $Obtain\_LUAP$, which requires retrieving the LUAPs from the $Local(sMAP)$. This will incur an execution cost of $O(|Neighbor(sMAP)| * Propagation\_time)$. Here, $|Neighbor(sMAP)|$ is the total number of neighbors of sMAP and $Propagation\_time$ is the round trip time for delivering $LUAP$ between two-hop neighboring MAPs.

We can also estimate the cache size upper bound for storing LUAP as follows. Let $Cache\_Size(MAP_i)$ be the cache size requirement for a specific MAP_i and Num_User be the maximum number of MUs associated to any MAP. Then we can obtain the upper bound for $Cache\_Size(MAP_i)$ by the following equation

$$\begin{aligned} & Cache\_Size(MAP_i) \\ \leq\ & Num\_User * |Neighbor(MAP_i)| * |LUAP| \end{aligned}$$

where $|Neighbor(MAP_i)|$ is the number of neighbors of MAP_i and $|LUAP|$ is the size of a LUAP.

Let (V, E) represent the Neighbor Graph of a WMN network, where $V = \{MAP_1, MAP_2, \ldots, MAP_n\}$ is the set of all MAPs in this domain and E is the set of all edges. Here, an edge $e_{i,j} = (MAP_i, MAP_j)$ means a reassociation exist between the MAP_i and MAP_j. Then we can obtain the overall memory upper bound of the caches in the whole WMN networks as follows:

$$\begin{aligned} & \sum_{MAP_i \in V} Cache\_Size(MAP_i) \\ \leq\ & Num\_User * |LUAP| * \sum_{MAP_i \in V} |Neighbor(MAP_i)| \\ =\ & Num\_User * |LUAP| * 2 * |E| \end{aligned}$$

Issuer	Receiver	$\mathcal{B}$	Enc(PMK)	SP	Exp	Sig

Fig. 2. The format of D-coin

E. D-coin Issuing and Inter-domain Handoff Phase

An inter-domain handoff means an active communication session changes its network attachment point from the serving domain to another one. Different from intra-domain handoff which can achieve fast intra-domain handoff authentication by pre-distributing the PMK one hop ahead of the MU [5], the inter-domain handoff involves not only the mutual authentication between the MU and the target WISP but also the inter-WISP payment issue. In SLAB, the inter-WISP authentication and billing can be realized with D-coin. Supposed that the remaining credit of the MU in the serving WISP domain is $\overline{\mathcal{B}}$, firstly, the MU will be collaboratively issued a piece of D-coin generated by the sMAP and the nMAPs.

A piece of D-coin is composed of seven components as shown in Fig. 2, where $Issuer$ is the current serving WISP, $Receiver$ is the tMAP of the handoff target WISP, $\overline{\mathcal{B}}$ represents not only the face value of this D-coin and the remaining credit of this MU but also the amount of this inter-WISP transaction, $Enc(PMK)$ refers to a new PMK between the MU and tWISP, which is encrypted with the tWISP's public key, SP is a hash chain newly generated by the MU as the spending proof described in Section III-C, Exp is the expiration date, and Sig is the issuer's signature on the above six components. Note that, D-coin can provide privacy preserving for MUs since the identity information of the MU is not included and then the MU can anonymously gain access to a foreign WISP domain. Among the seven components, a digital signature issued by the issuer plays a critical role

in building up the trust relationship among WISPs. In the following, we will show how a sMAP collaborates with its nMAPs to locally issue the D-coin.

Assume that every neighboring MAP periodically broadcasts its public key certificate along with service set identifier (SSID). After deciding the handoff target $MAP_{tMAP}@WISP_B$, the MU can easily authenticate the $tMAP$ by checking its public key certificate and CRL stored at the $sMAP$. After that, the MU generates a new hash chain $H^m(M')$ and derives a new PMK, which will be used to establish a secure channel with $tMAP_B$. MU encrypts the new PMK with $tMAP_B$'s public key and obtains $Enc(PMK)$. The encryption method can adopt any existing paring based encryption such as [22]. After that, MU sends a handoff request $hREQ = (tMAP@WISP_B, H^m(M'), Enc(PMK))$ to $sMAP_A$. $sMAP_A$ broadcasts this message to its one-hop neighbors and initializes the D-coin issuing algorithm in Algorithm 2.

Algorithm 2: Localized D-coin Issuing

Data: $(hREQ)$
Result: a valid D-coin
begin
  for *each* $MAP_A[i] \in \{sMAP_A, nMAP_As\}$ **do**
    Based on LUAP, summarize the MU's remaining credits $\overline{\mathcal{B}}$, generate a partial piece of D-coin by computing

$$Psig_i = s_i H_2(WISP_A||tMAP@WISP_B||\overline{\mathcal{B}}||H^m(M')||Enc(PMK)||Exp);$$

    Send $Psig_i$ to $sMAP_A$;
  end
  for $sMAP_A$ **do**
    Successfully collects k valid partial signatures (including the one generated by itself), denoted as $Psig_i$, $1 \le i \le k$;
    generate a full signature (D-coin) by computing

$$Sig = \sum_{i=1}^{k} \prod_{j=1, j\neq i}^{k} \frac{0-i}{j-i} \cdot Psig_i;$$

    Send Sig to the MU;
  end
  for *MU* **do**
    Obtain the Sig, check the validity by computing

$$\hat{e}(Sig, P^A) = \hat{e}(H_2(WISP_A||tMAP@WISP_B||\overline{\mathcal{B}}||H^m(M')||Enc(PMK)||Exp), Y^A);$$

    Get a full piece of D-coin $(WISP_A, tMAP@WISP_B, \overline{\mathcal{B}}, H^m(M'), Enc(PMK), Exp\ , Sig)$;
  end
  return D-coin
end

With valid D-coin, the MU can successfully handoff to the $tMAP$ operated by WISP B, where $tMAP$ only needs to verify the validity of the D-coin to ensure that this D-coin has not been spent before and decrypt the future pair-wise master key PMK from $Enc(PMK)$. Note that a double-spending check is critical to ensure the security of signature based authentication scheme since a digital signature can be used for more than once without such a check, which immediately leads to a service fraud. In addition, the double-spending check is normally performed by the RB, which will certainly cause extra delay. To avoid the centralized double-spending check, the proposed D-coin is localized by containing the name of $tMAP$ and its WISP. The localization of D-coin can effectively avoid the double-spending fraud by restricting the validity of the D-coin only within a specific MAP of the WISP domain. Therefore, the $tMAP$ only needs to maintain a local cache to check double-spending without going through the RB.

The above D-coin issuing and localized inter-domain handoff authentication scheme can be applied to not only the inter-domain handoffs between the home WISP domain and a foreign WISP domain but also the ones between two foreign WISPs. In the second case, the MU takes advantages of the D-coin to gain access to a foreign WISP domain, spend this D-coin as the protocols defined in Section III-C and collect another D-coin from this foreign network as defined in Section III-E before the next inter-domain handoff occurs. The above described procedure can be repeated until the roaming credits of this MU has run out or the MU is going to finish this inter-domain roaming by logging off. Before logging off, the MU can collect the remaining roaming credit by obtaining the last D-coin issued by the last foreign WISP. To transfer this D-coin to the home WISP of the MU, the identity of the home WISP is included in the D-coin as the receiver of this D-coin.

F. Clearance Phase

With the proposed SLAB scheme, the RB also serves as an Automated Clearing House (ACH) to enable the inter-WISP payment to be handled and processed in an efficient way. The SLAB clearance procedure is based on an event-driven model with batching, where every D-coin is regarded as an event while the D-coin can only be submitted to the RB when a batch of a given size of D-coin is gathered or after a minimum time period has elapsed. By dealing with a batch of clearance requests at a time, the centralized RB can be relieved from involving every inter-domain handoff and transaction. In addition, when the RB verifies the gathered D-coin, aggregate signature [12] is performed for reducing the transmission and verification cost. The following are the detailed clearance action steps:

Step 1: D-coin aggregation and submission

Let WISP B collect n pieces of D-coin from the same WISP A in the clearance phase: $D - coin_i = (WISP_A, T_i, Sig_i)$, where $i = 1, \cdots, n$ and $T_i = \{tMAP@WISP_B, \overline{\mathcal{B}}, H^m(M'), Enc(PMK), Exp\}$. Then, we can take advantage of the aggregate signature technique to merge the n pieces of D-coin into one single piece of D-coin by computing $\overline{Sig} = \prod Sig_i$. The aggregated D-coin can be represented as: $(WISP_A, T_1, \cdots, T_n, \overline{Sig})$. Then WISP B submits the aggregated D-coin as a clearance request to the RB.

Step 2: D-coin batch verification

After receiving the clearing request, the RB needs to verify the aggregate D-coin as follows:

1) Ensure that all the T_i are different and have not expired.
2) Batch the D-coin by further computing $\overline{T} = \prod_{i=1}^{n} H_2(WISP_A||tMAP_i@WISP_B||\overline{\mathcal{B}}_i||H^m(M_i')||Enc(PMK_i)||Exp_i)$.
3) Check the validity of the set of D-coin using the following equation: $\hat{e}(\overline{Sig}, P^A) = \hat{e}(\overline{T}, Y^A)$.

Step 3: Payments deposit

After ensuring the validity of the D-coin, the RB evaluates the amount of the D-coin by computing $\mathcal{B}_{sum} = \sum_{i=1}^{n} \overline{\mathcal{B}}_i$. A specific amount of money $\mathcal{B}_{sum}$ will be transferred from WISP A's account to WISP B's account. Thus, the inter-WISP payment between WISP A and B can be accomplished.

IV. Security analysis

A. Overall Security Improvement

With SLAB, the D-coin is issued under the endorsement of k or more than k neighboring MAPs. Let the number of MAPs in a WISP domain be n. In a normal case, a WISP is considered to be compromised as long as any registered MAP is compromised. On the other hand, with SLAB, a WISP is considered to be compromised only if k or more than k out of the totally n MAPs are simultaneously compromised, where the compromise resilience of the authentication and billing functionality can be further improved.

B. Compromised MAP attack

A compromised MAP may launch different attacks towards the MUs. In this section, we will discuss several compromised MAP related attacks and further show that the SLAB can thwart these attacks.

1) Prevention of D-coin Fraud Attack: A compromised MAP may launch the D-coin fraud attack by denying having accepted a piece of D-coin, and refuse to offer services to the MU, even the MAP did accept the D-coin. Furthermore, the compromised MAPs can sell the D-coin to other unauthorized MUs, which will lead to an immediate loss to the MUs. With SLAB, since an MU needs to submit the spending proofs (hash-chain tokens) on time to maintain a consistent session, even if a compromised MAP can fraud a piece of D-coin and transfer it to another unauthorized MU, the unauthorized D-coin holder cannot take advantage of this D-coin to gain access to the WMN without a valid usage proof on time. Since a session without submitting a spending proof will be terminated by the MGW, even if the compromised MAP frauds the D-coin at the authentication phase, the compromised MAPs cannot transfer it to the other MUs, by which the D-coin fraud attack can be thwarted.

2) Prevention of Overcharge Attack: The overcharge attack can be performed by a compromised MAP in such a way that the compromised MAP maliciously fails to inform the accounting server when the MU has disconnected from the MAP. The SLAB can successfully resist the overcharge attack due to the intrinsic non-repudiation feature. When an MU disconnects from an MAP, the MU will receive a D-coin indicating its remaining credits. Therefore, the D-coin can be utilized to resolve the possible dispute between MUs and WISPs resulting from overcharge attack.

C. Other Security Properties Discussion

1) Location Privacy Protection: Location privacy is another important issue related to roaming. In [21], the risks associated with the unauthorized disclosure, collection, retention, and usage of location data are discussed. A secure roaming scheme should be able to keep the MU's identity unknown to the foreign networks. In the proposed SLAB scheme, the MU's privacy can be well guaranteed through the employment of the D-coin since the identity information of its holder is not included.

2) Impersonation attack: A malicious attacker may impersonate a legitimate MAP and broadcast bogus beacons to attract the MUs. Therefore, mutual authentication is necessary. This can be achieved in the proposed SLAB scheme. In specific, when an MU sends a piece of D-coin to an MAP for authentication, the D-coin will include a PMK, which is encrypted with the public key of the MAP. The encrypted PMK, denoted as $Enc(PMK)$, can serve as a challenge by the MU to the MAP. Only a real MAP with the corresponding secret key can obtain the PMK by computing decryption operations so as to perform the subsequent re-association operation with the MU.

V. Performance Evaluation of The SLAB

The applicability of the SLAB scheme (denoted as **S**hort and **A**ggregate **S**ignature based SLAB, or SAS-SLAB) is evaluated through extensive simulation in terms of the inter-domain handoff delay and the workload at the RB. To further demonstrate the superiority of SLAB, we also evaluate a number of other existing inter-domain authentication solutions for comparison, including the IEEE 802.1x authentication scheme and public key certificate based localized authentication (PKC-LA) [7] [1]. It is worth noting that the proposed SLAB can achieve maximal flexibility by adopting different encryption and signature schemes as the building block. Therefore, we introduce two SLAB variations called RSA-SLAB and ECC-SLAB for comparison, which are based on RSA and ECC encryption and signature, respectively.

A. Average Inter-Domain Authentication Latency

In [24], the authentication latency is defined as the time from the instant when the MU sends an authentication request to the instant when the MU receives the authentication reply. Since inter-domain roaming is focused, the authentication latency can be expressed as

$$T_{AD}(i) = \overrightarrow{d} \cdot \overrightarrow{t} \tag{1}$$

where i is a specific inter-domain authentication scheme, $\overrightarrow{t}$ is a vector representing the authentication operations which may contribute to the authentication latency, and is defined as $\overrightarrow{t} = [T_{\mathsf{TR}}, T_{\mathsf{PK\_RSA}}, T_{\mathsf{PK\_ECC}}, T_{\mathsf{PK\_SAS}}, T_{\mathsf{PK\_PKC}}, T_{\mathsf{CRL}}]$, where all the time components are given in Table.I.

$\overrightarrow{d}$ is a vector denoting the amount of time for each time components. In the SAS-, RSA- and ECC-SLAB, the localized authentication is supported and thus the authentication

[1]In [7], there is no particular encryption or signature schemes defined. Without loss of generality, two classic encryption [22] and signature [23] are adopted as an example to evaluate the performance of PKC-LA.

TABLE I
EXPLANATION OF AUTHENTICATION LATENCY

Notation	Explanation
T_{TR}	Message transmission time on one hop
$T_{\mathsf{PK\_RSA}}$	RSA based Public Key Operation Time
$T_{\mathsf{PK\_ECC}}$	ECC based Public Key Operation Time
$T_{\mathsf{PK\_SAS}}$	Short Signature Based Public Key Operation Time
$T_{\mathsf{PK\_PKC}}$	ID-based Public Key Operation Time in Scheme PKC-LA.
T_{CRL}	Certificate Revocation List On-line Checking Time

message can traverse directly from the sMAP through the nMAP, sMAP and MU to the tMAP, which takes only 4 hops. Furthermore, SAS-, RSA- and ECC-SLAB also require 1 public key encryption, 1 decryption, 1 signature generation, and 2 verification operations based on pairing, RSA, and ECC, respectively. According to [7], the inter-domain authentication in PKC-LA is a three way handshake protocol. At each step, one signature or encrypted message is transmitted. Further, 2 signature generation/verification operations and 1 encryption/decryption need to be performed. In addition, one certificate revocation list checking operation is inevitable to defend the service abuse attack. Finally, in the IEEE 802.1x authentication scheme, the authentication request should be transmitted to the home network via N hops, and the home network will send the authentication result back via another N hops, where N refers to the distance between the sMAP and MU's home WISP. Notice that we do not take the symmetric key processing time into consideration since the running time of symmetric key is negligible compared with the other operations. Therefore, we have $\overrightarrow{d}$ as follows:

$$\begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \\ d_5 \end{pmatrix} = \begin{pmatrix} 4 & 0 & 0 & 1 & 0 & 0 \\ 2N & 0 & 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 1 & 1 \\ 4 & 1 & 0 & 0 & 0 & 0 \\ 4 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \tag{2}$$

To investigate the average inter-domain authentication delay, the mobility model in [25]–[27] is adopted. The probability density function (PDF) of the number of inter-domain handoff j can be written as follows:

$$\alpha(j) = \begin{cases} 1 - 1/\rho_{\mathsf{WISP}}[1 - f^*_{\mathsf{WISP}}(t)], & \text{if } j = 0, \\ 1/\rho_{\mathsf{WISP}}[1 - f^*_{\mathsf{WISP}}(t)]^2 * [f^*_{\mathsf{WISP}}(t)]^{i-1}, & \text{if } j > 0 \end{cases} \tag{3}$$

where residence time of the MU at a WISP follows a general distribution of $1/(\mu_{\mathsf{WISP}})$, its probability density function (PDF) is $f_{\mathsf{WISP}}(t)$ and Laplace transform is $f^*_{\mathsf{WISP}}(t)$. Let the inter-arrival time of each MU entering a network domain follow an exponential distribution with a mean of $1/\lambda$ and $\rho_{\mathsf{WISP}} = \lambda/\mu_{\mathsf{WISP}}$. The average authentication delay for any specific authentication scheme i can be defined as

$$T_{\mathsf{inter}}(i) = \sum_j \overrightarrow{d_i} \cdot \overrightarrow{t} \cdot j \cdot \alpha(j), \forall i = 1, 2, 3, 4, 5 \tag{4}$$

B. Parameter Setting

The parameter setting of the simulation is as follows. In IEEE 802.1x, the maximum authentication message is 4096 bytes, the transmission delay per hop is about 20 milliseconds

TABLE II
SUMMARY OF TRANSMISSION DELAY PER HOP IN DIFFERENT SCHEMES

	SAS-SLAB	IEEE 802.1x	PKC-LA	RSA-SLAB	ECC-SLAB
Delay/hop (ms)	0.5	20	0.2	1.5	0.6

TABLE III
SUMMARY OF VARIOUS PUBLIC KEY OPERATIONS COMPUTATION COST

	RSA	SAS	ECC	PKC-LA
Encrypt(ms)	0.03	1.3	1.55 (ECDH)	1.3
Decrypt(ms)	4.49	1.3	1.55 (ECDH)	1.3
Sign(ms)	4.49	1	1.55 (ECDSA)	1.3
Verify(ms)	0.03	1.3	1.95 (ECDSA)	2.6

provided with 2 Mbps link capacity [24]. The transmission delay per hop with different message sizes for each scheme is listed in Table. II. We evaluate the delay of cryptographic operations on an Intel Pentium 4 3.0 GHz machine with 1 GB RAM running Fedora Core 4 based on cryptographic library MIRACL [28] except the pairing operations. As reported in [29], by most efficient software optimization and hardware acceleration, the pairing calculation can be accomplished within 1.3 ms. Therefore, we can summarize various public key operations computation costs in Table III. Note that since the computation cost of the pairing based operations dominates the pairing-based public key process, we mainly consider the pairing calculation time.

According to [17], the latency incurred by the certificate revocation list checking is about 0.5s and the majority of it is from networks latency. All of the parameters to evaluate the authentication delay are summarized in Table IV.

We evaluate the effect of user mobility and the average hop count between each MAP and the MGW in terms of the average authentication latency. Fig. 3 shows the impact by varying the WISP domain residential time of each MU upon the average authentication latency, where the distance between an MAP and the MGW is 4. For the certificate revocation list checking operation, PKC-LA is subject to the longest authentication latency, followed by the IEEE 802.1x full authentication scheme. It can be seen that the proposed SAS-SLAB yields the shortest inter-domain handoff latency, while the authentication delay caused by two other SLAB variants are very close to each other. In addition, the average hop count between the MAPs and the MGW plays an important role in the average authentication delay when a centralized authentication method is in place. The delay of the full IEEE 802.1x authentication scheme increases significantly with the hop count from an MAP to the MGW. On the other hand, the hop count has very little impact on the authentication cost of the proposed SLAB schemes. This further demonstrates that achieving localized authentication could be very critical to seamless mobility support.

C. Workload on Roaming Broker

As for the load on RB, the advantage of the SLAB variants against IEEE 802.1x and PKC-LA is straightforward. IEEE 802.1x and PKC-LA require the RB to be online during an

TABLE IV
SUMMARY OF THE SIMULATION PARAMETERS

	T_{PK_RSA}	T_{PK_ECC}	T_{PK_SAS}	T_{PK_PKC}	T_{CRL}
Delay (ms)	9.07	8.55	6.2	9.1	500

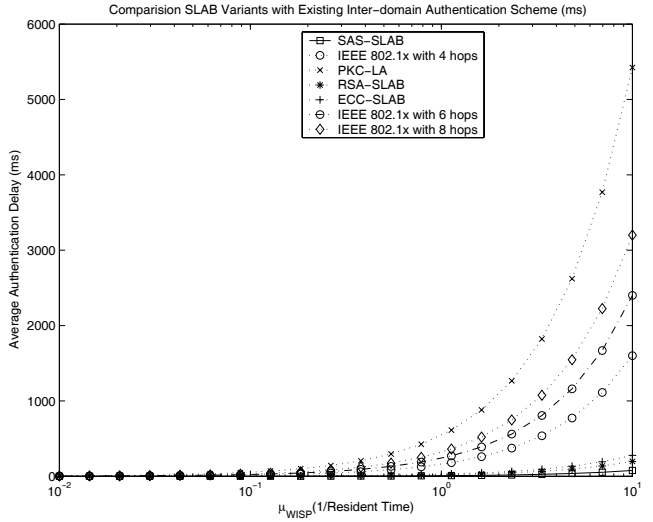


Fig. 3. Average authentication delay in different authentication schemes

TABLE V
THE SIZE OF EACH COMPONENT OF THE AUTHENTICATION MESSAGE IN SAS-SLAB (BYTES)

Components	Issuer	Receiver	$\mathcal{B}$	Enc()	SP	Exp	Sig
Size	8	8	8	40	8	20	8

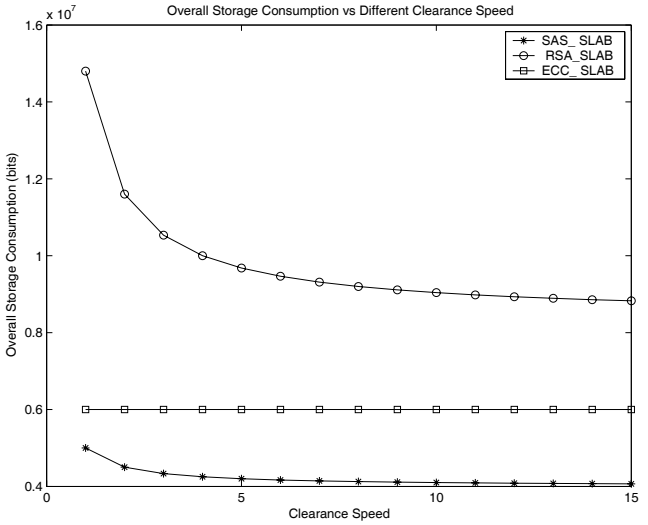


Fig. 4. Comparison of storage consumption on the RB under different SLAB schemes

inter-domain roaming event; while in SLAB, the inter-domain authentication and billing can be proceeded in a peer-to-peer fashion. However, it is not so obvious to see the advantages of the proposed SAS-SLAB over RSA-SLAB and ECC-SLAB in terms of load on RB. Therefore, in this section, we will examine the efficiency of the proposed SAS-SLAB scheme in terms of storage consumption and computation workload on RB. The following analysis will focus on SAS-, RSA- and ECC-SLAB schemes.

1) Space analysis: The approximate length of components of the D-coin in SAS-SLAB can be shown in V.

It is important to point out that by adopting the short signature technique [12], the signature field is only 20 bytes, which is much shorter than the length of a RSA and ECDSA signature which is 128 bytes and 40 bytes, respectively. By considering the public key encryption size, the size of a single D-coin in SAS-SLAB, RSA-SLAB and ECC-SLAB is 100, 296, and 120 bytes, respectively.

We further evaluate the overall storage consumptions for different schemes by considering the batch verification. Let the total number of D-coin be N and assume that a clearance action is automatically triggered when m pieces of D-coin are collected. Then the total storage consumption of the SAS-SLAB scheme can be computed as follows:

$$S_{SAS-SLAB} = 80N + 20N/m, 1 < m < N \tag{5}$$

According to [17], RSA also supports aggregation mode. Therefore, the total storage consumption of RSA-SLAB can be computed as

$$S_{RSA-SLAB} = 168N + 128N/m, 1 < m < N \tag{6}$$

However, the storage consumption in the ECC-SLAB scheme can be defined as

$$S_{ECC-SLAB} = 120N, 1 < m < N \tag{7}$$

For a large scale WMAN containing numerous independent MUs with frequent inter-domain transaction events, the storage saving achievement will yield great benefit. Suppose $N = 50,000$, we can manipulate the clearance speed in order to achieve desired storage consumption. The numerical results are shown in Fig. 4. It can be seen that once the clearance speed is set large enough (e.g., $m > 10$), SAS-SLAB can save about 33% and 50% storage consumption compared with that by ECC-SLAB and RSA-SLAB, respectively.

2) Computation workload for the RB: Similar to storage consumption, the aggregate technique may be employed to decrease the computation load of the RB. Assume that a WISP submits a piece of aggregate D-coin composed of N pieces of single D-coin. Before evaluating the computation workload on the RB, we need to breakdown the computation load of each algorithm and obtain the running time of each step. For the RSA scheme, when the public key e chooses a small prime such as 3, the aggregation cost of two signature operations is almost half of the RSA verification cost. Therefore, the overall RSA based aggregate verification on k distinct messages takes about $(k+1)/2$ times of verification for a piece of D-coin. For a short and aggregate signature, the aggregate verification cost only requires two pairing operations for multiple pieces of D-coin issued by the same WISP. We list the primitive computation cost for all the SLAB variants in Table VI.

Given a specific D-coin number N, we can obtain the computational cost on RB in different SLAB variants as shown in Fig. 5. It is observed that the performance of SAS-SLAB is also better than RSA-SLAB even when RSA-SLAB also supports aggregation operations.

TABLE VI
SUMMARY OF COMPUTATION COST OF VARIOUS SIGNATURE

	Verification cost for one signature	Aggregate Signing Cost (ms)
RSA (1024 bits)	0.03	$(k+1) \times 0.015$
SAS-SLAB (160 bits)	1.3	2×1.3
ECDSA (160bits)	1.95	$\times$

VI. DISCUSSIONS

A. Public Key Cryptography (PKC)

For minimizing the inter-domain handoff delay, this study provides a solution by reducing the transmission time in the authentication process at the expense of longer computation latency for public key processing. Under the PKI, the trust relationship can be initiated at the RB, and transferred to all the involved parties including every MAP, WISP, and MU, where an inter-domain handoff is simply treated as a cross-WISP transaction through issuing and reception of D-coin. Previously, the most common criticism on using PKC in wireless environment lies in the unacceptable computational complexity and communication overhead. However, recent rapid developments in improving the calculation speed and shortening the overhead of PKC have made it much more friendly in the application scenarios, where some well-known notoriously expensive cryptographic operations can be performed efficiently, such as pairing which took over 1 second to calculate when it was first invented. Currently, the hardware acceleration technique can deal with it within 1.3ms [29]. Therefore, the PKC based SLAB scheme can be a practical distributed security management solution in the application scenario of WMANs with through a WMN.

B. Distributed Security Management of WMN

Another unique feature of SLAB is its distributed security management. Although a centralized security management framework is still recommended by the IEEE (e.g., RADIUS) due to its highest security assurance, many academic researchers have argued that such a centralized scheme is not efficient and scalable when the network size is large [1], [10]. To achieve performance requirement, developing a security scheme that can initiate a graceful compromise between the performance and security assurance is highly desired and contributive. The proposed SLAB scheme is a fully distributed one, where the RB delegates its roaming functionalities to every WISP, which in turn delegates its security capabilities to every MAP in the whole WMN domain. Under a distribute security architecture, the bottleneck problem can be well resolved while an extremely high level of security guarantee can be achieved by way of a voting and threshold mechanism.

VII. CONCLUSIONS

We have proposed a novel secure localized authentication and billing (SLAB) scheme for service-oriented metropolitan-area WMNs. The scheme can successfully tackle the challenging tasks such as security guarantee and performance improvement in terms of system compromise resilience capability, inter-domain handoff authentication latency, and roaming broker's workload, etc. We have also demonstrated the practicality and feasibility of SLAB in a real-world application scenario of metropolitan-area wireless mesh networks. The research on other related security issues in WMNs, such as secure routing and mobility management, is underway.

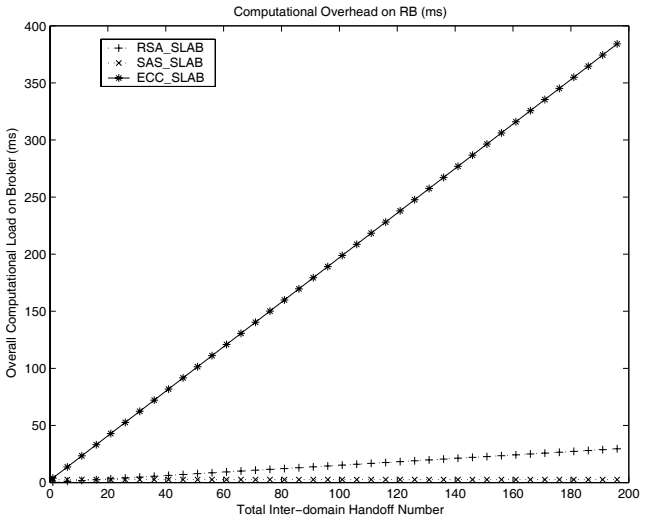


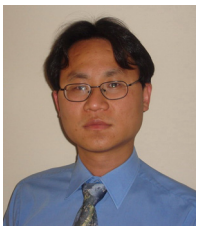
Fig. 5. Comparison of computational overhead on the RB in different schemes

REFERENCES

[1] I. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," *Computer Networks*, vol. 47, no. 4, pp. 445-487, Mar. 2005.
[2] C. de Laat, G. Gross, and L. Gommans, "Generic AAA architecture," Internet Draft, Mar. 2000.
[3] IEEE802.11s, http://grouper.ieee.org/groups/802/11/Reports/tgs_update.htm.
[4] S. Pack and Y. Choi, "Fast handoff scheme based on mobility prediction in public wireless LAN systems," *IEE Commun.*, vol. 151, no. 5, pp. 489-495, Oct. 2004.
[5] A. Mishra, M. H. Shin, N. L. Petroni, J. T. Clancy, and W. A. Arbauch, "Proactive key distribution using neighbor graphs," *IEEE Wireless Commun.*, vol. 11, no. 1, pp. 26-36, 2004.
[6] C. Chou and K. G. Shin, "An enhanced inter-access point protocol for uniform intra and intersubnet handoffs," *IEEE Trans. Mobile Comput.*, vol. 4, no. 4, pp. 321-334, July-Aug. 2005.
[7] Y. Zhang and Y. Fang, "ARSA: an attack-resilient security architecture for multi-hop wireless mesh networks," *IEEE J. Select. Areas Commun.*, vol. 24, no. 10, pp. 1916-1928, Oct. 2006.
[8] 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.
[9] M. Long, C. H. Wu, and J. D. Irwin, "Localised authentication for internetwork roaming across wireless LANs," *IEE Proc. Commun.*, vol. 151, no. 5, pp. 496-500, 2004.
[10] N. B. Salem and J. -P. Hubaux, "Securing wireless mesh networks," *IEEE Wireless Commun.*, vol. 13, no. 2, pp. 50-55, Apr. 2006.
[11] Z. Cao, H. Zhu, and R. Lu, "Provably secure robust threshold partial blind signature," *Science in China Series E*, vol. 35, no. 12, pp. 1254-1265, 2005.
[12] D. Boneh, B.Lynn, and H. Shacham, "Short signatures from the Weil pairing," *J. Cryptology*, vol. 17, no. 4, pp. 297-319, 2004.
[13] W. Liang and W. Wang, "A lightweight authentication protocol with local security association control in mobile networks," in *Proc. IEEE MILCOM'04*, Monterey, CA, USA, Oct. 2004.
[14] M. Shi, H. Rutagemwa, X. Shen, J. W. Mark, and A. Saleh, "A service agent based roaming architecture for WLAN/cellular integrated networks," accepted by *IEEE Trans. Veh. Technol*.
[15] Y. Zhang and Y. Fang, "A secure authentication and billing architecture for wireless mesh networks," *Wireless Networks*, vol. 13, no. 5, pp. 663-678, 2007.

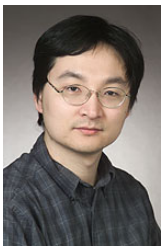
[16] H. Zhu, X. Lin, P.-H. Ho, X. Shen, and M. Shi,"TTP based privacy preserving inter-WISP roaming architecture for wireless metropolitan area networks," in *Proc. IEEE WCNC'07*, Hong Kong, Mar. 2007.
[17] M. Zhao, S. W. Smith, and D. M. Nicol, "Aggregated path authentication for efficient BGP security," in *Proc. CCS 2005*, pp. 128-138, Nov. 2005.
[18] L. Lamport, "Password authentication with insecure communication," *Commun. ACM*, vol. 24, no. 11, pp. 770-772, Nov. 1981.
[19] A. Mishra, M. H. Shin, and W. A. Arbauch,"Context caching using neighbour graphs for fast handoffs in a wireless network," in *Proc. IEEE INFOCOM'04*, Hong Kong, Mar. 2004.
[20] IEEE Std. 802.11i, "Draft Amendment to Standard for Telecommunications and Information Exchange between Systems-lan/man Specific Requirements, Part 11: Wireless Medium Access Control and Physical Layer (phy) Specifications: Medium Access Control (MAC) Security Enhancements.," May 2003.
[21] R. P. Minch, "Privacy issues in location-aware mobile devices," in *Proc. IEEE HICSS'04*, 2004.
[22] D. Boneh and M. Franklin, "Identify-based encryption from the Weil pairing," in *Proc. CRYPTO'01*, LNCS 2139, pp. 213-229, 2001.
[23] F. Hess, "Efficient identity based signature schemes based on pairings," in *Proc. SAC 2002*, LNCS 2595, pp. 310-324, 2003.
[24] W. Liang and W. Wang, "A quantitative study of authentication and QoS in wireless IP networks," in *Proc. IEEE INFOCOM'05*, Miami, FL, USA, Mar. 2005.
[25] S. Baek, S. Pack, T. Kwon, and Y. Choi, "A localized authentication, authorization, and accounting (AAA) protocol for mobile hotspots," in *Proc. WONS 2006*, 2006.
[26] Y. Fang, "Movement-based mobility management and trade off analysis for wireless mobile networks," in *IEEE Trans. Comput.*, vol. 52, no. 6, pp. 791-803, June 2003.
[27] Y. Fang, I. Chlamtac, Y. Lin, "Portable movement modeling for PCS networks," in *IEEE Trans. Veh. Technol.*, vol. 49, no.4, pp. 1356-1363, July 2000.
[28] Multiprecision Integer and Rational Arithmetic C/C++ Library (MIRACL).
[29] T. Kerins, W. P. Marnane, E. M. Popvici and P. S. L. M. Barreto, "Efficient hardware for the Tate pairing calculation in characteristic three," in *Proc. Workshop on Cryptographic Hardware and Embedded Systems 2005 (CHES 2005)*, Edinburgh, Scotland, Aug. 2005.

Haojin Zhu received his B.Sc. degree (2002) from Wuhan University (China) and his M.Sc. (2005) degree from Shanghai Jiao Tong University (China), both in computer science. He is currently working toward his Ph.D. degree in the electrical and computer engineering at the University of Waterloo, Waterloo, Canada. His current research interests include wireless network security and applied cryptography.



Xiaodong Lin (S'07) is currently working toward his Ph.D. degree in the Department of Electrical and Computer Engineering at the University of Waterloo, Ontario, Canada, where he is a Research Assistant in the Broadband Communications Research (BBCR) Group. His research interests include wireless network security, applied cryptography, and anomaly-based intrusion detection.

Rongxing Lu received the B.Sc. and M.Sc. degrees in computer science from the Tongji University, Shanghai, China, in 2000 and 2003, respectively. In 2006, he received the Ph.D degree in computer science from Shanghai Jiao Tong University, Shanghai, China. Currently, he is a Post-doctoral fellow at the University of Waterloo, Waterloo, Canada. His current research interests include wireless network security and cryptography. He is the co-recipient of IEEE ICC 2007 - Computer and Communications Secuity Symposium Best Paper Award.



Pin-Han Ho (M'04) received his B.Sc. and M.Sc. Degree from the Electrical and Computer Engineering department in the National Taiwan University in 1993 and 1995. He started his Ph.D. study in the year 2000 at Queens University, Kingston, Canada, focusing on optical communications systems, survivable networking, and QoS routing problems. He finished his Ph.D. in 2002, and joined the Electrical and Computer Engineering department in the University of Waterloo, Waterloo, Canada, as an assistant professor at the same year. Professor Pin-Han Ho is the author/coauthor of more than 100 refereed technical papers and book chapters, and the co-author of a book on optical networking and survivability. He is the recipient of Distinguished Research Excellent Award in the ECE department of University of Waterloo, Early Researcher Award (Premier Research Excellence Award) in 2005, the Best Paper Award in SPECTS'02, ICC'05 Optical Networking Symposium, and ICC'07 Security and Wireless Communications symposium, and the Outstanding Paper Award in HPSR'02.

Xuemin (Sherman) Shen (M'97-SM'02) 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/wireline 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 JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, 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.