

A Sophisticated Privacy-Enhanced Yet Accountable Security Framework for Metropolitan Wireless Mesh Networks

Kui Ren¹ and Wenjing Lou²

¹Department of ECE, Illinois Institute of Technology, Chicago, IL 60616, email: kren@ece.iit.edu

²Department of ECE, Worcester Polytechnic Institute, Worcester, MA 01609, email: wjlou@ece.wpi.edu

Abstract—Recently, multi-hop wireless mesh networks (WMNs) have attracted increasing attention and deployment as a low-cost approach to provide broadband Internet access at metropolitan scale. Security and privacy issues are of most concern in pushing the success of WMNs for their wide deployment and for supporting service-oriented applications. Despite the necessity, limited security research has been conducted towards privacy preservation in WMNs. This motivates us to develop PEACE, a sophisticated privacy-Enhanced yet Accountable seCurity framEwork, tailored for WMNs. At the one hand, PEACE enforces strict user access control to cope with both free riders and malicious users. On the other hand, PEACE offers sophisticated user privacy protection against both adversaries and various other network entities. PEACE is presented as a suite of authentication and key agreement protocols built upon our proposed short group signature variation. Our analysis shows that PEACE is resilient to a number of security and privacy related attacks.

I. INTRODUCTION

Wireless mesh networks (WMNs) have recently attracted increasing attention and deployment as a promising low-cost approach to provide last-mile high-speed Internet access at metropolitan scale [1], [2]. Typically, a WMN is a multi-hop layered wireless network as shown in Fig. 1 [3], [4]. The first layer consists of access points which are high-speed wired Internet entry points. At the second layer, stationary mesh routers form a multihop backbone via long-range high-speed wireless techniques such as WiMAX [5]. The wireless backbone connects to wired access points at some mesh routers through high-speed wireless links. The third layer consists of a large number of mobile network users. These network users access the network either by a direct wireless link or through a chain of other peer users to a nearby mesh router. WMNs represent *a unique marriage of the ubiquitous coverage of wide-area cellular networks with the ease and the speed of local-area Wi-Fi networks* [3]. The advantages of WMNs also include low deployment costs, self-configuration and self-maintenance, good scalability, high robustness, etc. [1].

Security and privacy issues are of most concern in pushing the success of WMNs for their wide deployment and for supporting service-oriented applications. Due to the intrinsically open and distributed nature of WMNs, it is essential to enforce network access control to cope with both free riders and malicious attackers. Dynamic access to WMNs should be subject to successful user authentication based on the properly

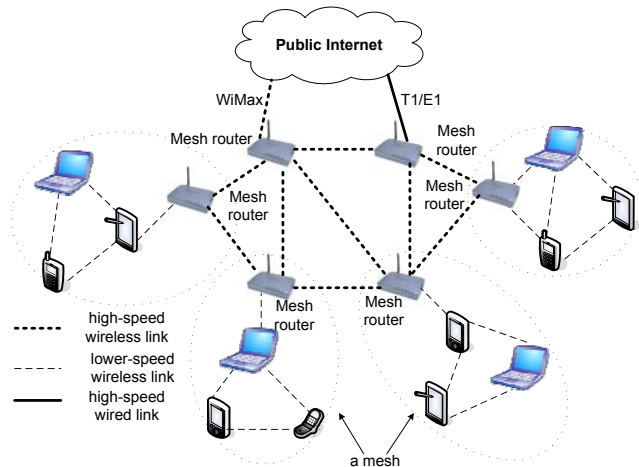


Fig. 1. WMN network architecture [3], [4]

preestablished trust between users and the network operator; otherwise, network access should be prohibited. On the other hand, it is also critical to provide adequate provisioning over user privacy as WMN communications usually contain a vast amount of sensitive user information. The wireless medium, open network architecture, and lack of physical protection over mesh routers render WMNs highly vulnerable to various privacy-oriented attacks. These attacks range from passive eavesdropping to active message phishing, interception, and alteration, which could easily lead to the leakage of user information. Obviously, the wide deployment of WMNs can succeed only after users are assured for their ability to manage privacy risks and maintain their desired level of anonymity.

The necessity of security and privacy in WMNs can be well illustrated through the following example. In a metro-scale community mesh network, the citizen access WMNs from everywhere within the community such as offices, homes, restaurants, hospitals, hotels, shopping malls, and even vehicles. Through WMNs they access the public Internet in different roles and contexts for services like emails, e-banking, e-commerce, and web surfing, and also interact with their local peers for file sharing, teleconferencing, online gaming, instant chatting, etc. Integrated with sensors and cameras, the WMN may also be used to collect information of interest. In fact, at

Boston suburb area, the City of Malden [6], the police department will use the WMN “to stream video footage from local areas directly to the police station, making it easier for police officers to monitor and respond to crimes at those locations.” [6] Obviously, all these communications contain various kinds of sensitive user information like personal identities, activities, location information, financial information, transaction profiles, social/business connections, and so on. Once disclosed to the attackers, these information could compromise any user’s privacy and, when further correlated together, can cause even more devastating consequences. Hence, securing user privacy is of paramount practical importance in WMNs. Moreover, for both billing purpose and avoiding abuse of network resources, it is also essential to prohibit free riders and let only legitimate residences access WMNs.

Despite the necessity and importance, limited research has been conducted to address privacy-enhanced security mechanisms in WMNs. This motivates us to propose PEACE, a sophisticated privacy-Enhanced yet Accountable seCurity framEwork for WMNs. Our contribution are four-fold:

Security: It achieves explicit mutual authentication and key establishment between users and mesh routers and between users and mesh routers themselves. It thus prohibits both illegal network access from free riders and malicious users and phishing attacks due to rogue mesh routers.

Anonymity: It simultaneously enables unilateral anonymous authentication between users and mesh routers and bilateral anonymous authentication between any two users. It thus ensures user anonymity and privacy.

Accountability: It enables user accountability, aimed at regulating user behaviors and protecting WMNs from being abused and attacked. Network communications can always be audited in the cases of disputes and frauds. It further allows dynamic user revocation so that malicious users can be evicted.

Sophisticated User Privacy: It allows users to disclose minimum information possible while maintaining accountability. In PEACE, the user identity is a multi-faceted information as network users as society members always interact with WMNs in different roles and contexts. Therefore, a dispute regarding a given communication session should only be attributed to the according role/context information of the user without disclosing his full identity information (unless necessary).

To our best knowledge, PEACE is the first attempt to establish an accountable security framework with a sophisticated privacy protection model tailored for WMNs. PEACE also lays a solid background for designing other upper layer security and privacy solutions, e.g., anonymous communication.

The rest of the paper is organized as follows. Section II is the introduction of the cryptographic knowledge entailed by PEACE. Section III is the problem formulation. Then, in Section IV, the details of PEACE are described. We further analyze in Section V the security and privacy properties of PEACE, as well as its performance. Section VI is related work. Finally, we conclude our paper in Section VII.

II. THE CRYPTOGRAPHIC BACKGROUND

A. Bilinear Groups

We first introduce a few concepts related to bilinear maps as they are important to the design of PEACE. Let $\mathbb{G}_1, \mathbb{G}_2$ be multiplicative cyclic groups generated by g_1 and g_2 , respectively, whose orders are a prime p , and \mathbb{G}_T be a cyclic multiplicative group with the same order p . Suppose there is an efficient and computable isomorphism $\psi : \mathbb{G}_2 \rightarrow \mathbb{G}_1$ such that $\psi(g_2) = g_1$. Let $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ be a bilinear pairing with the following properties [7]:

- **Bilinearity:** $e(aP, bQ) = e(P, Q)^{ab}$ for all $P \in \mathbb{G}_1, Q \in \mathbb{G}_2, a, b \in \mathbb{Z}_p$
- **Non-degeneracy:** $e(g_1, g_2) \neq 1$
- **Computability:** There is an efficient algorithm to compute $e(P, Q)$ for all $P \in \mathbb{G}_1, Q \in \mathbb{G}_2$

B. Group Signature

Group signature schemes are a relatively recent cryptographic concept introduced by Chaum and van Heyst in 1991 [8]. A group signature scheme is a method for allowing a member of a group to sign a message on behalf of the group. In contrast to ordinary signatures, it provides anonymity to the signer, i.e., a verifier can only tell that a member of some group signed. However, in exceptional cases such as a legal dispute, any group signature can be “opened” by a designated group manager to reveal unambiguously the identity of the signature’s originator. Some group signature schemes support revocation, where group membership can be disabled. One of the most recent group signature schemes is the one proposed by Boneh and Shacham [7], which has a very short signature size that is comparable to that of an RSA-1024 signature [9]. This scheme is based on the following two problems that are believed to be hard. Let $\mathbb{G}_1, \mathbb{G}_2, g_1, g_2$ as defined above.

q -Strong Diffie-Hellman Problem: The q -SDH problem in $(\mathbb{G}_1, \mathbb{G}_2)$ is defined as follows: given a $(q + 2)$ -tuple $(g_1, g_2, g_2^\gamma, g_2^{\gamma^2}, \dots, g_2^{\gamma^q})$ as input, output a pair $(g_1^{1/(\gamma+x)}, x)$, where $x \in \mathbb{Z}_p^*$.

Decision Linear on \mathbb{G}_1 : Given arbitrary generators u, v, h of \mathbb{G}_1 and $u^a, v^b, h^c \in \mathbb{G}_1$ as input, output **yes** if $a + b = c$ and **no** otherwise.

III. PROBLEM FORMULATION

A. Network Architecture and System Assumptions

The three-layer architecture in Fig. 1 considers a metropolitan-scale WMN under the control of a network operator (*NO*). The network operator deploys a number of APs and mesh routers and forms a well connected WMN that covers the whole area of a city and provides network services to network users, i.e., the citizens. Network users, on the other hand, subscribe to the network operator for the services and utilize their mobile clients to freely access the network from anywhere within the city. The membership of network users may be i) terminated/renewed according to user-operator agreement in a periodic manner, or ii) dynamically revoked by *NO* in case of dispute/attack.

Similar to [3], [10], we assume that the downlink from a mesh router to all users within its coverage is one hop. However, the uplink from a user to a mesh router may be one or multiple hops. That is, a network user needs to transmit packets in multiple hops to a mesh router beyond his direct transmission range. In this case, network users cooperate with each other on relaying the packets to mesh routers. We further assume that all the network traffic has to go through a mesh router except the communication between two direct neighboring users. We assume so as it is expected that communications to and from a mesh router will constitute the majority of traffic in a WMN [11]. Moreover, this assumption would significantly reduce the routing complexity from the users' point of view as mesh routers will take the responsibility.

We assume that *NO* can always communicate with mesh routers through pre-established secure channels, and so are mesh routers themselves. The WMN is assumed to be deployed with redundancy in mind so that revocation of individual mesh routers will not affect network connection. We assume the existence of an off-line trusted third party (*TTP*), which is trusted for not disclosing the information it stores. *TTP* is required only during the system setup. We further assume that there is a secure channel between *TTP* and each network user.

B. Threat Model and Security Requirements

Due to the open medium and spatially distributed nature, WMNs are vulnerable to both passive and active attacks. The passive attacks include eavesdropping, while active attacks range from message replaying, bogus message injection, phishing, active impersonation to mesh router compromise. Hence, for a practical threat model we consider an adversary that is able to eavesdrop all network communications, as well as inject arbitrary bogus messages. In addition, the adversary can compromise and control a small number of users and mesh routers subject to his choices; it may also set up rogue mesh routers to phish user accesses. The purposes of the adversary include i) gain illegal and unaccountable network access, ii) intrude the privacy of legitimate network users, and iii) launch denial-of-service (DoS) attacks against service availability.

In light of the above threat model, the following security requirements are essential to ensure a WMN function correctly and securely as purposed.

- *User-router mutual authentication and key agreement*: A mesh router and a user should mutually authenticate each other to prevent both unauthorized network access and phishing attacks. The user and the mesh router should also establish a shared pairwise symmetric key for session authentication and message encryption.
- *User-user mutual authentication and key agreement*: Users should also authentication each other before co-operation in regards to message relaying and routing. Moreover, symmetric keys should be established and effectively maintained to provide session authentication and message encryption over the corresponding traffic.
- *Sophisticated User Privacy Protection*: The privacy of users should be well protected, and we differentiate user

privacy against different entities such as the adversary, *NO*, and the law authority, as will be elaborated below in Section II.C.

- *User accountability*: In the cases of attacks and disputes, the responsible users and/or user groups should be able to audited and pinpointed. On the other hand, no innocent users can be framed for disputes/attacks they are not involved in.
- *Membership Maintenance*: The network should be able to handle membership dynamics including membership revocation, renewing, and addition.
- *DoS resilience*: The WMN should maintain service availability despite of DoS attacks.

C. Privacy Model

In a metropolitan WMN, city residences as network users access the WMN for services related to every aspect of their personal and professional lives. Inevitably, these network communications will contain a large amount of personal, business, and organization information that are highly sensitive and interested by different parties for different purposes. The malicious adversaries are interested as they could gain economic benefits by stealing the identity and other information. In fact, identity theft has been an infamous type of the Internet crimes. Furthermore, network communications accumulated over time and space may be intentionally collected and used for establishing user profiles by certain parties, including *NO*. These parties are not necessarily malicious, but such actions certainly violate user privacy. Obviously, the success deployment of WMNs is subject to users' assurance of their ability to manage privacy risks and maintain their desired level of anonymity.

The above observation leads to the establishment of a practical user privacy model which provides sophisticated user privacy management and addresses user accountability simultaneously. We observe that a user usually accesses the WMN in different roles and under different contexts. For example, a user as an engineer may access the WMN in his office as an employee of a company. The same user may also access the WMN from a university campus as a student, from a rented apartment as a tenant, and from a golf club as a paid member, and so on. In our privacy model, we hence refer to the *user identity* as a user's collective attribute information according to his different roles in the society. In the above example, the user identity may include

{*name, ssn, engineer of company X, tenant of apartment Y, student of university Z, member of golf club V, ...*}.

Formally, we can divide the user identity information into two different categories, that is, *essential attribute information* and *nonessential attribute information* as shown in Fig. 2. The *essential attribute information* includes all the information that can be used uniquely identify a specific user such as user's name, social security number, driver license number, passport number, etc. On the other hand, the *nonessential attribute information* of a user may include his different social roles as indicated in the above example. We note that if *essential*


 User Identity	Essential Attribute Information	Name
		Social Security Number
		Driver License Number
		State ID
	Nonessential Attribute Information	Social Role 1
		Social Role 2
		Social Role 3
	
		Social Role i
	

Fig. 2. The format of user identity information

attribute information of a user are disclosed, this user is fully exposed and all his attribute information will also be disclosed. On the other hand, disclosing nonessential attribute information does not lead to the full exposure of the user's identity. That is, a user can still maintain a certain level of anonymity, when only his nonessential attribute information is disclosed. It is further observed that the nonessential attribute information of users are still sufficient for accountability purpose from *NO*'s perspective. This is because *NO* can still enforce network access control and audit network communications as it makes no difference to *NO* whether or not a responsible entity is a person, a company or an organization.

To protect user privacy, the user identity information should be well protected from network communications against the adversary and even *NO*. Therefore, it should be required that i) *no communication sessions should reveal any user identity information except that the user is a legitimate network user*; ii) *no entity including the adversary and NO could link two different communication sessions to the same particular user*. Furthermore, in the cases of disputes and attacks, user privacy should be protected against *NO* in such a way that iii) *a given communication session under audit by NO can only be linked to the according attribute information of the user without disclosing his full identity information*. That is, only minimum necessary identity information is disclosed for the security purpose so that user privacy can be best protected.

Our privacy model further considers the extreme cases such as severe attacks in which the law authority has to track the particular responsible attacker. For this purpose, we introduces the concept of *user group* and try to utilize the natural society hierarchy among network users. A *user group* refers to any society entity, which, through a *user group manager*, manages a certain number of network users, i.e., its staffs and/or employees, and subscribes network services on behalf of its users. A *user group* can be any company, organization, university, or government agency, etc. A network user, on the other hand, usually belongs to multiple different *user groups* according to his roles in the society. In our privacy model, we further require that iv) *only by joint effort from both a user group manager and NO can a user's full identity be disclosed; and neither of them can do so alone*. Note that the capability of a *user group manager* itself is strictly restricted, that is, it has no more ability than an ordinary network user. *User group managers* cannot link any communication session to a specific user by only themselves.

In summary, our privacy model is aimed at the following

privacy guarantees under the threat model discussed above.

- Against the adversary, the *user group managers*, and other entities (except *NO* and the law authority): At no circumstances the adversary could tell that two different communication sessions are from the same network user or link a communication session to a specific user.
- Against *NO*: Given any communication session, *NO* can only tell which user group the corresponding user is from, but cannot recover user's full identity. That is, *NO* can only recover the corresponding nonessential user attribute information for the accountability purpose.
- Against the law authority: With the help from both *NO* and *user group managers*, the law authority could link any communication session to the corresponding network user that is responsible.

IV. PEACE: THE SCHEME

When designing PEACE, we find that none of current privacy-aware digital signature primitives, such as blind signature, ring signature, and group signature schemes, suits our purpose given the security and privacy requirements discussed above. Blind signature and ring signature schemes can only provide irrevocable anonymity, while PEACE demands user accountability and hence revocable anonymity. Existing group signature schemes do provide revocable anonymity, but can not support sophisticated user privacy. This motivates us to tailor a group signature scheme to meet all the requirements. We hence develop a variation of the short group signature scheme proposed in [7] by modifying its key generation algorithm for our purpose. PEACE is then built on this new group signature variation by further integrating it into the authentication and key agreement protocol design.

A. Scheme Setup

The following setup operations are performed in an off-line manner by all the entities in PEACE, namely, *NO*, a trusted third party (*TTP*), mesh routers, network users, and user group managers. PEACE works under bilinear groups $(\mathbb{G}_1, \mathbb{G}_2)$ with isomorphism ψ and respective generators g_1 and g_2 , as in Section II.A. PEACE also employs hash functions H_0 and H , with respective ranges \mathbb{G}_2^2 and \mathbb{Z}_p . Notation below mainly follow [7].

NO is responsible for key generation operation. Specifically, *NO* proceeds as follows:

- 1) Select a generator g_2 in \mathbb{G}_2 uniformly at random, and set $g_1 \leftarrow \psi(g_2)$. Select $\gamma \xleftarrow{R} \mathbb{Z}_p^*$ and set $w = g_2^\gamma$.
- 2) Select $\text{grp}_i \xleftarrow{R} \mathbb{Z}_p^*$ for a registered user group i .
- 3) Using γ , generate an SDH tuple $(A_{i,j}, \text{grp}_i, x_j)$ by selecting $x_j \xleftarrow{R} \mathbb{Z}_p^*$ such that $\gamma + \text{grp}_i + x_j \neq 0$, and setting $A_{i,j} \leftarrow g_1^{1/(\gamma + \text{grp}_i + x_j)}$.
- 4) Repeat Step 3) for a predetermined number of times that are mutually agreed by *NO* and the user group manager GM_i .
- 5) Send $GM_i \{[i, j], \text{grp}_i, x_j \mid \forall j\}$ via a secure channel.
- 6) Repeat Steps 2), 3), and 4) for every user group.

7) Send $TTP: \{[i, j], \mathbf{A}_{i,j} \oplus \mathbf{x}_j \mid \forall i, j\}$ via a secure channel, where \oplus denotes bitwise *exclusive OR* operation¹.

The above operation generates the group public key, gpk , and a number of private keys, gsk .

$$\begin{cases} gpk = (g_1, g_2, w), \\ \{gsk[i, j] = (\mathbf{A}_{i,j}, \mathbf{grp}_i, \mathbf{x}_j) \mid \forall i, j\} \end{cases}$$

Furthermore, NO obtains a set of revocation token, grt , with $grt[i, j] = \mathbf{A}_{i,j}$ and also keeps the mapping between group id i and \mathbf{grp}_i for all user groups. Note that γ is the system secret only known to NO . For the purpose of non-repudiation, NO signs on Steps 5) and 7) under a standard digital signature scheme, such as ECDSA [12]. In PEACE, we assume ECDSA-160 is used. For the same purpose, GM_i and TTP also sign on these messages upon receipt and sends the resulted signature back to NO .

Additionally, NO prepares each mesh router MR_k a public/private key pair, denoted as $(\mathbf{RPK}_k, \mathbf{RSK}_k)$. Each mesh router also obtains an accompanied public key certificate signed by NO to prove key authenticity. The signing key pair of NO is denoted as $(\mathbf{NPK}, \mathbf{NSK})$. The certificate contains the following fields at the minimum:

$$Cert_k = \{\mathbf{MR}_k, \mathbf{RPK}_k, ExpT, Sig_{\mathbf{NSK}}\},$$

where $ExpT$ is the expiration time, and Sig_{\bullet} denotes an ECDSA-160 signature signed on a given message using a private key \bullet .

Before accessing the WMN, a network user has to authenticate himself to his belonging user groups². From each such user group i , a network user uid_j is assigned a random group private key as follows:

- 1) GM_i sends uid_j ($[i, j], \mathbf{grp}_i, \mathbf{x}_j$) as well as the related system parameters.
- 2) GM_i requests TTP to send uid_j ($[i, j], \mathbf{A}_{i,j} \oplus \mathbf{x}_j$) by providing the index $[i, j]$.
- 3) uid_j assembles his group private key as $gsk[i, j] = (\mathbf{A}_{i,j}, \mathbf{grp}_i, \mathbf{x}_j)$.

Note that in our setting,

- GM_i only keeps the mapping of $(uid_j, (\mathbf{grp}_i, \mathbf{x}_j))$ but has no knowledge of the corresponding $\mathbf{A}_{i,j}$.
- NO only knows the mapping of $(GM_i, gsk[i, j])$ but has no knowledge regarding to whom $gsk[i, j]$ is assigned.
- TTP has the mapping of $(uid_j, (\mathbf{A}_{i,j} \oplus \mathbf{x}_j, \mathbf{grp}_i))$ as it sends uid_j this information through a secure channel between the two upon the request from GM_i . But TTP has no knowledge of the corresponding \mathbf{x}_j or $\mathbf{A}_{i,j}$.

Here, we use uid_j representing the user's essential attribute information. For the purpose of non-repudiation, uid_j signs on the messages he receives from GM_i and TTP under ECDSA-160, and sends back GM_i the corresponding signature.

¹ \mathbf{x}_j might have a larger bitlength as compared to $\mathbf{A}_{i,j}$, which is a point on the chosen elliptic curve. In this case, we simply ignore the unnecessary bits of \mathbf{x}_j .

²Such authentication is based on the pre-established trust relationship between the user and the user group and may be done through in-person contact.

B. User-router Mutual Authentication and Key Agreement

To access the WMN, a network user follows the user-router mutual authentication and key agreement protocol as specified below, when a mesh router is within his direct communication range³.

- 1) The mesh router MR_k first picks a random nonce $r_R \xleftarrow{R} \mathbb{Z}_p^*$ and a random generator g in \mathbb{G}_1 and then computes g^{r_R} . MR_k further signs on g, g^{r_R} , and current timestamp \mathbf{ts}_1 , using ECDSA-160. MR_k then broadcasts

$$g, g^{r_R}, \mathbf{ts}_1, Sig_{\mathbf{RSK}_k}, Cert_k, CRL, URL \quad (M.1)$$

as part of *beacon messages* that are periodically broadcasted to declare service existence. Here, CRL and URL denote the mesh router certificate revocation list and the user revocation list, respectively. Specifically, URL contains a set of revocation tokens that corresponds to the revoked group private keys, which is a subset of grt . Both CRL and URL are signed by NO .

- 2) Upon receipt of (M.1), a network user uid_j proceeds as follows:

- 2.1) Check the timestamp \mathbf{ts}_1 to prevent replay attack.

Examine $Cert_k$ to verify public key authenticity and the certificate expiration time; examine CRL and see if $Cert_k$ has been revoked by applying \mathbf{NPK} ; Further verify the authenticity of $Sig_{\mathbf{RSK}_k}$ by applying \mathbf{RPK}_k .

- 2.2) Upon positive check results, uid_j believes that MR_k is legitimate and does the following.

- 2.2.1) Pick two random nonce $r, r_j \xleftarrow{R} \mathbb{Z}_p$, compute g^{r_j} , and prepare the current timestamp \mathbf{ts}_2 . Further obtain two generators (\hat{u}, \hat{v}) in \mathbb{G}_2 from H_0 as

$$(\hat{u}, \hat{v}) \leftarrow H_0(gpk, g^{r_j}, g^{r_R}, \mathbf{ts}_2, r) \in \mathbb{G}_2^2 \quad (Eq.1)$$

and compute their images in \mathbb{G}_1 : $u \leftarrow \psi(\hat{u})$ and $v \leftarrow \psi(\hat{v})$.

- 2.2.2) Compute $T_1 \leftarrow u^\alpha$ and $T_2 \leftarrow \mathbf{A}_{i,j} v^\alpha$ by selecting an exponent $\alpha \xleftarrow{R} \mathbb{Z}_p$. Set $\delta \leftarrow (\mathbf{grp}_i + \mathbf{x}_j)^\alpha \in \mathbb{Z}_p$. Pick blinding values r_α, r_x , and $r_\delta \xleftarrow{R} \mathbb{Z}_p$.

- 2.2.3) Compute helper values R_1, R_2 , and R_3 : $R_1 \leftarrow u^{r_\alpha}$, $R_2 \leftarrow \hat{e}(T_2, g_2)^{r_x} \cdot e(v, w)^{-r_\alpha} \cdot e(v, g_2)^{-r_\delta}$, and $R_3 \leftarrow T_1^{r_x} \cdot u^{-r_\delta}$. Compute a challenge value $c \in \mathbb{Z}_p$ using H :

$$c \leftarrow H(gpk, g^{r_j}, g^{r_R}, \mathbf{ts}_2, r, T_1, T_2, R_1, R_2, R_3) \in \mathbb{Z}_p.$$

- 2.2.4) Compute $s_\alpha = r_\alpha + c\alpha$, $s_x = r_x + c(\mathbf{grp}_i + \mathbf{x}_j)$, and $s_\delta = r_\delta + c\delta \in \mathbb{Z}_p$. Obtain the group signature on $\{g^{r_j}, g^{r_R}, \mathbf{ts}_2\}$ as

$$SIG_{gsk[i,j]} \leftarrow (r, T_1, T_2, c, s_\alpha, s_x, s_\delta).$$

- 2.2.5) Compute the shared symmetric key with MR_k :

$$K_{k,j} = (g^{r_R})^{r_j}.$$

³If direct communication is not possible due to lack of mobility, a user can increase transmit power to reach the mesh router during this phase. After this phase, the user should reduce transmit power back to the normal level to help increase spatial concurrency and frequency reuse [3]

2.3) Unicast back to MR_k

$$g^{r^j}, g^{r^R}, \mathbf{ts}_2, \widehat{SIG}_{gsk[i,j]}. \quad (M.2)$$

3) Upon receipt of (M.2), MR_k carries out the following to authenticate uid_j :

3.1) Check g^{r^R} and \mathbf{ts}_2 to make sure the freshness of (M.2).

3.2) Check that $\widehat{SIG}_{gsk[i,j]}$ is a valid signature by applying the group public key gpk as follows.

3.2.1) Compute \hat{u} and \hat{v} using (Eq.1), and their images u and v in \mathbb{G}_1 : $u \leftarrow \psi(\hat{u})$ and $v \leftarrow \psi(\hat{v})$.

3.2.2) Retrieve R_1, R_2 , and R_3 as: $\tilde{R}_1 \leftarrow u^{s_\alpha}/T_1^c$, $\tilde{R}_2 \leftarrow e(T_2, g_2)^{s_x} \cdot e(v, w)^{-s_\alpha} \cdot e(v, g_2)^{-s_\delta} \cdot (e(T_2, w)/e(g_1, g_2))^c$, and $\tilde{R}_3 \leftarrow T_1^{s_x} \cdot u^{-s_\delta}$.

3.2.3) Check that the challenge c is correct:

$$c \stackrel{?}{=} H(gpk, g^{r^j}, g^{r^R}, \mathbf{ts}_2, r, T_1, T_2, \tilde{R}_1, \tilde{R}_2, \tilde{R}_3). \quad (Eq.2)$$

3.3) For each revocation token $A \in URL$, check whether A is encoded in (T_1, T_2) by checking if

$$e(T_2/A, \hat{u}) \stackrel{?}{=} e(T_1, \hat{v}) \quad (Eq.3)$$

If no revocation token of URL is encoded in (T_1, T_2) , the signer of $\widehat{SIG}_{gsk[i,j]}$ has not been revoked.

If all above checks succeed, MR_k is now assured that the current user is a legitimate network user, although MR_k does not know which particular user this is. Note that uid_j is never disclosed or transmitted during protocol execution.

3.4) MR_k further computes the shared symmetric key as $K_{k,j} = (g^{r^j})^{r^R}$ and send back uid_j :

$$g^{r^j}, g^{r^R}, E_{K_{k,j}}(MR_k, g^{r^j}, g^{r^R}), \quad (M.3)$$

where $E_\bullet(\cdot)$ denotes symmetric encryption of the given message within the brackets using key \bullet .

The above protocol enables explicit mutual authentication between a mesh router and a legitimate network user; it also enables unilateral anonymous authentication for the network user. Upon successful completion of the protocol, the mesh router and the user also establish a shared symmetric key used for the subsequent communication session. And this session is uniquely identified through (g^{r^R}, g^{r^j}) .

C. User-user Mutual Authentication and Key Agreement

In PEACE, neighboring legitimate network users may help to relay each other's traffic. To this end, two network users within each other's direct communication range first authenticate each other and establish shared secret pairwise key as follows:

1) uid_j picks a random nonce $r_j \xleftarrow{R} \mathbb{Z}_p^*$ and computes g^{r^j} , where g is obtained from the *beacon messages* broadcasted by the current service mesh router. uid_j further signs on g, g^{r^j} , and current timestamp \mathbf{ts}_1 , using his group private key $gsk[i, j]$ following Steps 2.2.1) to 2.2.4) as in Section IV.B. uid_j then locally broadcasts

$$g, g^{r^j}, \mathbf{ts}_1, \widehat{SIG}_{gsk[i,j]} \quad (\widetilde{M}.1)$$

2) Upon receipt of $(\widetilde{M}.1)$, uid_i checks the timestamp and verifies the authenticity of $\widehat{SIG}_{gsk[i,j]}$ by applying the group key gpk following Step 3.2) as in Section IV.B. uid_i further check if the signature is generated from a revoked group private key following Step 3.3) as in Section IV.B. Note that URL can always be obtained from the *beacon messages*.

If all checks succeed, uid_i is assured that the current user it communicates with is legitimate. uid_i proceeds to pick a random nonce $r_l \xleftarrow{R} \mathbb{Z}_p^*$ and computes g^{r_l} . uid_i further signs on g^{r^j}, g^{r_l} , and current timestamp \mathbf{ts}_2 , using an appropriate group private key $gsk[t, l]$ of his. uid_i also computes the shared pairwise session key as $K_{r_j, r_l} = (g^{r^j})^{r_l}$. uid_i then replies uid_j

$$g^{r^j}, g^{r_l}, \mathbf{ts}_2, \widehat{SIG}_{gsk[t,l]} \quad (\widetilde{M}.2)$$

3) Upon receipt of $(\widetilde{M}.2)$, uid_j first checks whether $\mathbf{ts}_2 - \mathbf{ts}_1$ is within the acceptable delay window. uid_j also examines $\widehat{SIG}_{gsk[i,j]}$ and URL as uid_i did above. If all checks succeed, uid_j is also assured that its communicating counterpart is legitimate. uid_j computes the shared pairwise session key as $K_{r_j, r_l} = (g^{r_l})^{r_j}$. uid_j finally replies uid_i

$$g^{r^j}, g^{r_l}, E_{K_{r_j, r_l}}(g^{r^j}, g^{r_l}, \mathbf{ts}_1, \mathbf{ts}_2) \quad (\widetilde{M}.3)$$

Upon receipt of $(\widetilde{M}.3)$ and successful decryption of $E_{K_{r_j, r_l}}(g^{r^j}, g^{r_l}, \mathbf{ts}_1, \mathbf{ts}_2)$, uid_i is assured that uid_j has successfully completed the authentication protocol and established the shared key for their subsequent communication session, which is uniquely identified through (g^{r^j}, g^{r_l}) .

D. Privacy-Enhanced User Accountability

This design of PEACE protects user privacy in a sophisticated manner, while still maintaining user accountability.

User anonymity against the adversary, the user groups, and TTP. In PEACE, a user only authenticates himself as a legitimate service subscriber without disclosing any of his identity information by utilizing the group signature technique. Neither the adversary nor the user group managers can tell which particular user generates a given signature. The adversary, even by compromising mesh routers and other network users, that is, knowing a number of group private keys in addition to the group public key, still cannot deduce any information regarding the particular group private key used for signature generation. This is due to the hardness of the underlying q -SDH problem, where q is a 1020-bit prime number. Due to the same reason, neither a user group manager can distinguish whether or not one of his group members has signed a particular signature as he has no knowledge of the corresponding $A_{i,j}$ s nor can he compute them. The same conclusion also holds for TTP as TTP can compute neither x_j nor $A_{i,j}$ given $A_{i,j} \oplus x_j$. Furthermore, every data session in PEACE is identified only through pairs of fresh random numbers, which again discloses nothing regarding user identity

information [13]. In addition, PEACE requires a network user to refresh session identifiers and the shared symmetric keys for each different session. This further eliminates the linkability between any two sessions initiated by the same network user. We note that even with the help of compromised mesh routers and other network users, the adversary still cannot judge whether two communication sessions are from the same user. This is because, fundamentally, none of them can tell whether two signatures are from the same user, given q -SDH problem and decision linear on \mathbb{G}_1 problem are hard.

User privacy against NO and user accountability: Since NO knows grt , it can always tell which $gsk[i, j]$ produces a given signature. However, NO has no knowledge regarding to whom $gsk[i, j]$ is assigned as PEACE allows a late binding between group private keys and network users. Furthermore, it is user group managers' sole responsibility to assign group private keys to each network user without any involvement of NO. Therefore, NO could only map $gsk[i, j]$ to the user group i based on grp_i . Because no other entities except NO and the key holder himself has the knowledge of the corresponding $A_{i,j}$ and can therefore generate the given signature, the key holder must be a member of user group i . This audit result serves our both requirements. On the one hand, the result only reveals partial nonessential attribute information of the user and still protects user privacy to an extent. On the other hand, the result is sufficient for user accountability purposes for NO.

When NO (on behalf of mesh routers) finds certain communication session disputable or suspicious, it conducts the following protocol to audit the responsible entity.

1. Given the link and the session identifier, find the corresponding authentication session message $(M.2) = g^{r_j}, g^{r_R}, ts_2, SIG_{gsk[i,j]}$ from the network log file.
2. For each revocation token $A_{i,j} \in grt$, check whether $e(T_2/A_{i,j}, \hat{u}) \stackrel{?}{=} e(T_1, \hat{v})$. Output the first element $A_{i,j} \in grt$ such that $e(T_2/A_{i,j}, \hat{u}) = e(T_1, \hat{v})$.
3. For the found revocation token $A_{i,j}$, output the corresponding mapping between $A_{i,j}$ and grp_i . Since grp_i maps to a particular user group i , now a responsible entity is found from the perspective of NO.

From the user's perspective, only part of his nonessential attribute information is disclosed from the audit. But such nonessential attribute information will not reveal his essential attribute information. For example, the above audit may find the responsible user is a member of Company XYZ but cannot reveal any other information regarding the user. Yet NO still has sufficient evidence to prove to Company XYZ that one of his members violates certain network access rule so that Company XYZ should take the corresponding responsibility specified in their service subscription agreement.

Revocable user anonymity against law authority: When law authority decides to track the particular attacker that is responsible for a certain communication session, the following procedure is taken: NO reports to the law authority $(A_{i,j}, grp_i)$ by executing the above protocol against the session in audit. $(A_{i,j}, grp_i)$ is then further forwarded to GM_i . GM_i checks its local record, finds out the mapping between $(grp_i$ and $x_i)$

and hence the corresponding user identity information uid_j , to whom $gsk[i, j]$ is assigned during the system setup. GM_i then replies uid_j to law authority. At this point, law authority and only law authority gets to know about which particular user is responsible for the communication session in audit. We point out this tracing procedure has the non-repudiation property because i) GM_i signed on all gsk s that are assigned from NO as the proof of receipt; ii) uid_j also signed on the messages when obtaining $gsk[i, j]$ from GM_i and TTP as the proof of receipt. PEACE also has non-frameability property because no one else knows $gsk[i, j]$ except NO and uid_j or is able to forge a signature on behalf of uid_j .

V. SCHEME ANALYSIS

A. System Security Analysis: As its fundamental security functionality, PEACE enforces network access control. Hence, we are most concerned with the following three different types of attacks, i.e., bogus data injection attacks, data phishing attacks, and DoS attacks.

Bogus Data Injection Attacks: In such attacks, the adversary wants to inject bogus data to the WMN aimed at utilizing the network service for free. The sources of the bogus data could be outsiders, revoked users, or revoked mesh routers. However, such bogus data traffic will be all immediately filtered in PEACE. Firstly, with respect to outsiders they do not know any group private keys. Thus, they cannot produce correct message signatures, when attempting to initialize a communication session with NO and/or other network users. They also cannot bypass the authentication procedure and directly send out bogus data to others as they do not possess any shared symmetric session keys with them and thus cannot produce correct MACs. Next, regarding revoked users, there are two situations: i) they do not have any group private key currently in use due to group public key update; or ii) the corresponding group private keys owned by them are already revoked and are published in *URL* in beacon messages. Obviously, the revoked users cannot gain network access in neither cases. Lastly, for revoked mesh routers, they are no longer valid members of the WMN. By checking *CRL*, no legitimate mesh routers will accept/relay data traffic from revoked mesh routers. Also, since the downlink from a mesh router to its service range is only one hop, network users never need to and will not relay data traffic for mesh routers in PEACE.

Data Phishing Attacks: In such attacks, the adversary may set up bogus mesh routers and try to phish user connections to such routers. In this way, the adversary could control network connection and analyze users' data traffic for their benefits. The phishing mesh routers can be either completely new mesh routers or revoked mesh routers both at the adversary's control. In the former case, the mesh router will not be able to authenticate itself to the network user. Therefore, no network user will establish any session with such a mesh router. Even if the mesh router could intercept the network traffic between a network user and a legitimate mesh router, it will not be able to decrypt the message and obtain any useful information. In the latter case, a newly revoked mesh router, however, will

possibly be able to authenticate itself to a network user, if such a user does not possess the latest version of *CRL*. The network user may be cheated in this case but only for up to (inverse of the update frequency – (current time – last periodical update time)) time period. This is because the revoked mesh router will not be able to provide a legal *CRL* update at the next periodical *CRL* update time point.

DoS Attacks: In such attacks, the adversary may flood a large number of illegal access request messages to mesh routers. The purpose is to exhaust their resources and render them less capable of serving legitimate users. In PEACE, for every access request message (*M.2*), the corresponding mesh router has to verify a group signature and check the validity of the signer. Both operations involve expensive pairing operations, which hence can be easily exploited by the adversary. To deal with this issue, we adopt the same client-puzzle approach as adopted in [14]. The idea of this approach is as follows: When there is no evidence of attack, a mesh router processes (*M.2*) normally. But when under a suspected DoS attack, the mesh router will attach a cryptographic puzzle to every (*M.1*) and requires the solution to the puzzle be attached to each (*M.2*). The mesh router commits resources to process (*M.2*) only when the solution is correct. Typically, solving a client puzzle requires a brute-force search in the solution space, while solution verification is trivial [14]. Therefore, the adversary must have abundant resources to be able to promptly compute a large enough number of puzzle solutions in line with his sending rate of bogus access request (*M.2*). By contrast, although puzzles slightly increase legitimate users' computational load when the mesh router is under attack, they are still able to obtain network accesses regardless the existence of the attack. We refer the readers to [14] for the complete design.

B. User Privacy and Accountability Analysis: PEACE protects user privacy in a sophisticated manner, while still maintaining user accountability. Firstly, PEACE enables user anonymity against the adversary, the user group managers, and *TTP*. In PEACE, a network user only authenticates himself as a legitimate service subscriber without disclosing any of his identity information by utilizing the group signature technique. Neither the adversary nor the user group managers can tell which particular user generates a given signature. The adversary, even by compromising mesh routers and other network users, that is, knowing a number of group private keys in addition to the group public key, still cannot deduce any information regarding the particular group private key used for signature generation. This is due to the hardness of the underlying q -SDH problem, where q is a 1020-bit prime number. Due to the same reason, a user group manager also cannot distinguish whether or not one of his group members has signed a particular signature as he has no knowledge of the corresponding $A_{i,j}$ s nor can he compute them. The same conclusion also holds for *TTP* as *TTP* can compute neither x_j nor $A_{i,j}$ given $A_{i,j} \oplus x_j$. Furthermore, every data session in PEACE is identified only through pairs of fresh random

numbers, which again discloses nothing regarding user identity information. In addition, PEACE requires a network user to refresh session identifiers and the shared symmetric keys for each different session. This further eliminates the linkage between any two sessions originated from the same network user. We note that even with the help of compromised mesh routers and other network users, the adversary still cannot judge whether two communication sessions are from the same user. This is because, fundamentally, none of them can tell whether two signatures are from the same user, given q -SDH problem and decision linear on \mathbb{G}_1 problem are hard.

Secondly, PEACE provides sufficient user privacy protection against *NO* while maintaining user accountability. Since *NO* knows *grt*, it can always tell which $gsk[i, j]$ produces a given signature. However, *NO* has no knowledge regarding to whom $gsk[i, j]$ is assigned as PEACE allows a late binding between group private keys and network users. Furthermore, it is user group managers' sole responsibility to assign group private keys to each network user without any involvement of *NO*. Therefore, *NO* could only map $gsk[i, j]$ to the user group i based on grp_i . Because no other entities except *NO* and the key holder himself has the knowledge of the corresponding $A_{i,j}$ and can therefore generate the given signature, the key holder has to be a member of user group i . This audit result serves our both requirements. On the one hand, the result only reveals partial nonessential attribute information of the user and still protects user privacy to an extent. On the other hand, the result is sufficient for user accountability purposes for *NO*.

Lastly, PEACE provides revocable user anonymity against the law authority. As discussed in Section IV.D, the law authority could track any particular user through the cooperation from both *NO* and the corresponding user group manager.

C. Performance Analysis:

Communication Overhead: In PEACE, Both authentication and key agreement protocols require only three-way communication between mesh routers and network users and between network users. This is the minimal communication rounds necessary to achieve mutual authentication, and therefore PEACE incurs a reduced authentication delay. Furthermore, by design PEACE poses minimum additional communication overhead on network users as they may carry their mobile clients such as PDAs and smart phones other than laptops to access the WMN. These mobile clients are much less powerful as compared to mesh routers with regard to their communication capability. In messages (*M.1*), (*M.1*), and (*M.2*), a network user only needs to transmit a group signature to fulfill the authentication function. As we base our group signature variation on the scheme proposed in [7], the signature comprises two elements of \mathbb{G}_1 and five elements of \mathbb{Z}_p . When using the curves described in [15], one can take p to be a 170-bit prime and use a group \mathbb{G}_1 where each element is 171 bits. Thus, the total group signature length is 1,192 bits or 149 bytes. With these parameters, security is approximately the same as a standard 1024-bit RSA signature, which is 128 bytes [7]. That is, the length of the group signature is almost the same as that of a standard RSA-1024 signature.

Computational Overhead: In PEACE, the most computationally expensive operations are the signature generation and verification. Signature generation requires two applications of the isomorphism ψ . Computing the isomorphism takes roughly the same time as an exponentiation in \mathbb{G}_1 (using fast computations of the trace map) [7]. Thus, signature generation requires about 8 exponentiations (or multiexponentiations) and 2 bilinear map computations. Signature verification takes 6 exponentiations and $3 + 2|URL|$ computations of the bilinear map. By design, PEACE adopts an asymmetric-symmetric hybrid approach for session authentication to reduce computational cost. Network entities (both mesh routers and mesh routers) execute expensive group signature operation to authenticate each other only when establishing a new session; all subsequent data exchanging of the same session is authenticated through highly efficient MAC-based approach.

More specifically, PEACE requires a network user executing exactly one signature generation and one signature verification when performing mutual authentication for establishing a new session. It can be seen that the actually computational cost of signature verification depends on the size of URL , while signature generation cost is fixed. PEACE can proactively control the size of URL as described in [13]. Moreover, a far more efficient revocation check algorithm, whose running time is independent of $|URL|$ can be adopted as described in [7] with a little bit sacrifice on user privacy. This technique could further bring the total cost of signature verification to 6 exponentiations and 5 bilinear map computations. On the other hand, PEACE requires a mesh router to perform mutual authentication with every network user within its coverage for each different session and sign on every beacon message being periodically broadcasted.

VI. RELATED WORK

Security research in WMNs is still in its early stage, especially with respect to user privacy protection. [16] discusses specifics of WMNs and identifies fundamental network operations that need to be secured. [17] surveys the threats and vulnerabilities faced by WMNs and also identified a number of security goals. [18] discussed a security architecture for WMNs based on IEEE 802.1X. [4] and [3] discuss how to support secure user roaming in a number of WMNs belonging to different domains. [19] present an anonymous routing scheme for static WMNs. [20], [21] presents an authentication scheme for WMNs which is resilient against mesh router compromise. Other general privacy-aware authentication techniques include [22], [23]. A full version of this paper can be found in [13].

VII. CONCLUSION

In this paper, we proposed PEACE, which, to our best knowledge, is the first attempt to establish an accountable security framework with a sophisticated user privacy protection model tailored for metropolitan scale WMNs. We developed a variation of the short group signature scheme [7]. We then built PEACE on this new signature variation by further integrating it into the authentication and key agreement protocol design.

At the one hand, PEACE enforces strict user access control to cope with both free riders and malicious users. On the other hand, PEACE offers sophisticated user privacy protection against both adversaries and various other network entities. Our analysis showed that PEACE is resilient to a number of security and privacy related attacks.

ACKNOWLEDGEMENT

This research is supported in part by ERIF, IIT and National Science Foundation Grants CNS-0626601 and CNS-0716306.

REFERENCES

- [1] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: A survey," *Computer Networks*, Mar. 2005.
- [2] "Self organizing neighborhood wireless mesh networks," <http://www.research.microsoft.com/mesh/>.
- [3] Y. Zhang and Y. Fang, "A secure authentication and billing architecture for wireless mesh networks," *ACM Wireless Networks*, to Appear.
- [4] —, "Arsa: an attack-resilient security architecture for multi-hop wireless mesh networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 10, pp. 1916–1928, Oct. 2006.
- [5] "The wimax forum," <http://www.wimaxforum.org>.
- [6] "Boston suburb secures metro-scale wireless mesh network with bluesocket," <http://www.tmcnet.com/usubmit/2006/09/27/1936581.htm>, Sept. 2006.
- [7] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in *ACM conference on Computer and Communications Security (CCS)*, 2004, pp. 168–177.
- [8] D. Chaum and E. van Heyst, "Group signatures," in *Proceedings of Eurocrypt, LNCS*, vol. 547, 1991, pp. 257–265.
- [9] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2.
- [10] M. Jakobsson, J. Hubaux, and L. Buttyan, "A charging and rewarding scheme for packet forwarding in multi-hop cellular networks," in *7th Int. Conf. Financial Cryptography (FC'03)*, 2003.
- [11] N. Salem, L. Buttyan, J. Hubaux, and M. Jakobsson, "A micro-payment scheme encouraging collaboration in multi-hop cellular networks," in *ACM MobiHoc*, 2003.
- [12] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. Springer-Verlag, 2004.
- [13] K. Ren and W. Lou, "A sophisticated privacy-enhanced yet accountable security framework for wireless mesh networks," in *Technical Report*, 2008.
- [14] A. Juels and J. Brainard, "Client puzzles: A cryptographic countermeasure against connection depletion attacks," in *6th NDSS*, 1999.
- [15] D. Boneh, H. Shacham, and B. Lynn, "Short signatures from the weil pairing," *Journal of Cryptology*, vol. 17, no. 4.
- [16] N. Ben Salem and J.-P. Hubaux, "Securing Wireless Mesh Networks," *IEEE Wireless Communications*, vol. 13, no. 2, 2006.
- [17] M. Siddiqui and C. Hong, "Security issues in wireless mesh networks," in *IEEE intl. conf. on multimedia and ubiquitous engineering*, 2007.
- [18] A. Cheikhrouhou and H. Chaouchi, "Security architecture in a multi-hop mesh network," in *5th conf. on security architecture research*, 2006.
- [19] X. Wu and N. Li, "Achieving privacy in mesh networks," in *ACM SASN*, 2006.
- [20] X. Lin, R. Lu, P.-H. Ho, X. Shen, and Z. Cao, "Tua: A novel compromise-resilient authentication architecture for wireless mesh networks," *IEEE Transactions on Wireless Communications*, To Appear.
- [21] X. Lin, X. Ling, H. Zhu, P.-H. Ho, and X. Shen, "A novel localized authentication scheme in IEEE 802.11 based wireless mesh networks," *International Journal of Security and Networks*, vol. 3, no. 2, pp. 122–132, 2008.
- [22] K. Ren, W. Lou, K. Kim, and R. Deng, "A novel privacy preserving authentication and access control scheme for pervasive computing environment," *IEEE Transactions on Vehicular Technology (TVT)*, vol. 55, no. 4, pp. 1373–1384, July 2006.
- [23] K. Ren and W. Lou, "Privacy-enhanced, attack-resilient access control in pervasive computing environments with optional context authentication capability," *ACM Mobile Networks and Applications (MONET) (special issue on Wireless Broadband Access)*, vol. 12, pp. 79–92, 2007.