A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks

Jinyuan Sun, Chi Zhang and Yuguang Fang
Department of Electrical and Computer Engineering
University of Florida, Gainesville, USA
{stellas@, zhangchi@, fang@ece.}ufl.edu

***Abstract*—Anonymity has received increasing attention in the literature due to the users' awareness of their privacy nowadays. Anonymity provides protection for users to enjoy network services without being traced. While anonymity related issues have been extensively studied in payment-based systems such as e-cash [1] and peer-to-peer (P2P) [2] systems, little effort has been devoted to wireless mesh networks (WMNs). On the other hand, the network authority requires conditional anonymity such that misbehaving entities in the network remain traceable. In this paper, we propose a security architecture to ensure unconditional anonymity for honest users and traceability of misbehaving users for network authorities in WMNs. The proposed architecture strives to resolve the conflicts between the anonymity and traceability objectives, in addition to guaranteeing fundamental security requirements including authentication, confidentiality, data integrity, and non-repudiation [3]. Further security enhancements can be incorporated, rendering the proposed architecture conditionally anonymous in terms of network access activities, location information, and communication paths.**

I. Introduction

Wireless Mesh Network (WMN) is a promising technology and is expected to be widespread due to its low-investment feature and the wireless broadband services it supports, attractive to both service providers (SPs) and users. However, security issues inherent in WMNs or any wireless networks need be considered before the deployment and proliferation of these networks, since it is unappealing to subscribers to obtain services without security and privacy guarantees. Wireless security has been the hot topic in the literature for various network technologies such as cellular networks [4], wireless local area networks (WLAN) [5], wireless sensor networks [6], [7], mobile ad hoc networks (MANETs) [8], [9], and vehicular ad hoc networks (VANETs) [10]. Recently, new proposals on WMN security [11], [12] have emerged. In [11], the authors describe the specifics of WMNs and identify three fundamental network operations that need to be secured. We [12] propose an attack-resilient security architecture (ARSA) for WMNs, addressing countermeasures to a wide range of attacks in WMNs. Due to the fact that security in WMNs is still in its infancy as very little attention has been devoted so far [11], a majority of security issues have not been addressed and are surveyed in [13].

Anonymity and privacy issues have gained considerable research effort in the literature [1], [2], [10], [12] [14]- [22], which have focused on investigating anonymity in different context or application scenarios. One requirement for anonymity is to unlink a user's identity to his or her specific activities, such as the anonymity fulfilled in the untraceable e-cash systems [1], [14] and the P2P payment systems [2], [15], where the payments cannot be linked to the identity of a payer by the bank or broker. Anonymity is also required to hide the location information of a user to prevent movement tracing, as is important in mobile networks [16]- [18] and VANETs [10]. In wireless communication systems, it is easier for a global observer to mount traffic analysis attack by following the packet forwarding path than in wired networks. Thus, routing anonymity [19]- [22] is indispensable which conceals the confidential communication relationship of two parties by building an anonymous path between them. Nevertheless, unconditional anonymity may incur insider attacks since misbehaving users are no longer traceable. Therefore, traceability is highly desirable such as in e-cash systems [1], [14] where it is used for detecting and tracing double-spenders.

In this paper, we are motivated by resolving the above security conflicts, namely, anonymity and traceability, in the emerging WMN communication systems. Our system borrows the blind signature technique from payment systems [1], [2], [15], [23] and hence can achieve the anonymity of unlinking user identities from activities, as well as the traceability of misbehaving users. Furthermore, the proposed pseudonym technique renders user location information unexposed. Our work differs from previous work in that, WMNs have unique hierarchical topologies and rely heavily on wireless links, which have to be considered in the anonymity design. As a result, the original anonymity scheme for payment systems among bank, customer, and store cannot be directly applied. In addition to the anonymity scheme, other security issues such as authentication, key establishment, and revocation are also critical in WMNs to ensure the correct application of the anonymity scheme. Moreover, although we employ the widely used pseudonym approach to ensure network access anonymity and location privacy, our pseudonym generation does not rely on a central authority, *e.g.*, the broker in [12], the domain authority in [16], the transportation authority or the manufacturer in [10], the trusted authority in [19], *etc*, who can derive the user's identity from his pseudonyms and illegally trace an honest user. Note that our system is not intended for achieving routing anonymity, which can be incorporated as an enhancement. Specifically, our major contributions in this paper include: 1) design of a ticket-based anonymity system with traceability property; 2) binding of the ticket and pseudonym which guarantees anonymous access control (*i.e.*, authentication of a user at the access point) and simplified revocation process; 3) adoption of the hierarchical ID-based cryptography for inter-domain authentication avoiding domain parameter certification.

II. PRELIMINARIES

A. *IBC FROM BILINEAR PAIRINGS*

ID-based cryptography (IBC) allows the public key of an entity to be derived from its public identity information such as name, email address, *etc*, which avoids the use of certificates for public key verification in the conventional PKI (public key infrastructure) [24]. Boneh and Franklin [25] introduced the first functional and efficient ID-based encryption scheme based on bilinear pairings on elliptic curves. Specifically, let G_1 and G_2 be an additive group and a multiplicative group, respectively, of the same prime order q. Discrete logarithm problem (DLP) is assumed to be hard in both G_1 and G_2. Let P denote a random generator of G_1 and $e : G_1 \times G_1 \rightarrow G_2$ denote a bilinear map constructed by modified Weil or Tate pairing with the following properties:

1) Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$, $\forall P, Q \in G_1$ and $\forall a, b \in Z_q^*$.
2) Non-degenerate: $\exists P, Q \in G_1$ such that $e(P, Q) \neq 1$.
3) Computable: there exists an efficient algorithm to compute $e(P, Q), \forall P, Q \in G_1$.

B. *BLIND SIGNATURE CRYPTOSYSTEMS*

Blind signature cryptosystems were first introduced by Chaum [23]. In general, a blind signature scheme allows a receiver to obtain a signature on a message such that both the message and the resulting signature remain unknown to the signer. We refer the readers to [26] for a formal definition of a blind signature scheme, which should bear the properties of verifiability, unlinkability, and unforgeability according to [23].

Brands [27] developed the first restrictive blind signature scheme, where the restrictiveness property is incorporated into the blind signature scheme such that the message being signed must contain encoded information. Partial blind signature schemes [28], [29] allow the resulting signature to convey publicly visible information on common agreements between the signer and the receiver. Partially restrictive blind signature schemes [30]–[32] were derived from the aforementioned work. They are essentially blind signature schemes with restrictiveness and partial blindness properties. In the restrictive partially blind signature schemes [31], [32] that serve as a building block for our architecture, the two key concepts, namely, restrictiveness and partial blindness, are defined based on [1], [28] (refer to [31], [32] for formal definitions).

III. SYSTEM MODEL

A. *NOTATION AND DEFINITIONS*

1) *NOTATION:*

- $\rightarrow$, $\rightarrow\rightarrow$, and $\|$: denote single-hop communications, multi-hop communications, and concatenation, respectively.
- CL, MR, GW, and TA: abbreviations for client, mesh router, gateway, and trusted authority, respectively.
- ID_x: the real identity of an entity x in our WMN system.
- PS_x: the pseudonym self-generated by a CL x by using its real identity ID_x.
- $H_1(M)$ and $H_1'(M)$: $\{0,1\}^* \rightarrow G_1$, cryptographic hash functions mapping an arbitrary string M to G_1.
- H_2: a cryptographic secure hash function: $G_1^3 \times G_2^5 \rightarrow Z_q$.
- H_3: a cryptographic secure hash function: $G_2 \times G_2 \times ID_{GW} \times date/time \rightarrow Z_q$.
- $H_1(ID_x)/\Gamma_x$ and $H_1(IDT_x)/\psi_x$: the public/private key pairs assigned to an entity x in the standard IBC and the hierarchical IBC, respectively.
- $PS_x/\widetilde{\Gamma_x}$ and $PST_x/\widetilde{\psi_x}$: the self-generated pseudonym/ private key pairs based on the above public/private key pairs.
- $\mathcal{SIG}_{\Gamma_x}(m)$: the ID-based signature on a message m using the signer x's private key Γ_x.
- $\mathcal{VER}(\mathcal{SIG})$: the verification process of the above signature which returns "accept" or "reject".
- $\mathcal{HIDS}_{\psi_x, s_x}(m)$: the hierarchical ID-based signature on a message m generated by the signer x using its secret point ψ_x and secret number s_x for inter-domain authentication.
- $\mathcal{HVER}(\mathcal{HIDS}, QT)$: the verification process using the above $\mathcal{HIDS}$ and QT which returns "accept" or "reject".
- $\mathcal{SKE}_\kappa(D)$: the symmetric key encryption on plaintext D using the shared secret key κ.
- $\mathcal{HMAC}_\kappa(m)$: the keyed-hash message authentication code on a message m using cryptographic hash functions and the symmetric key κ.

2) *DEFINITIONS:*

- *Anonymity (Untraceability)*: The anonymity of a legitimate CL refers to the untraceability of the CL's network access activities. The CL is said to be anonymous if the TA or the GW, or even the collusion of the two cannot link the CL's network access activities to the CL's real identity.
- *Traceability*: A legitimate CL is said to be traceable if the TA is able to link the CL's network access activities to the CL's real identity *if and only if* the CL misbehaves, *i.e.*, one or both of the following occurs: ticket-reuse and multiple-deposit.
- *Ticket-reuse*: one type of misbehavior of a legitimate CL that refers to the CL's use of a depleted ticket (*val*=0).
- *Multiple-deposit*: one type of misbehavior of a legitimate CL that refers to the CL's disclosure of its valid ticket and associated secrets to unauthorized entities or CLs with non-conformed behavior, so that these coalescing CLs can gain network access from different GWs simultaneously.
- *Collusion*: the colluding of malicious TA and GW to trace a legitimate CL's network access activities in the TA's domain (*i.e.*, to compromise the CL's anonymity).
- *Framing*: a type of attack mounted by a malicious TA in order to revoke a legitimate CL's network access privilege. In this attack, the TA can generate a false account number and associate it with the CL's identity. The TA can then create valid tickets based on the false account number and commit fraud (*i.e.*, misbehave). By doing so, the TA is able to falsely accuse the CL to have misbehaved and to revoke its access right.

B. NETWORK ARCHITECTURE

Consider the network topology of a typical WMN depicted in Fig. 1. The wireless mesh backbone consists of mesh routers (MRs) and gateways (GWs) interconnected by ordinary wireless links (shown as dashed curves). MRs and GWs serve as the access points (APs) of the WMN and the last resorts to the Internet, respectively. The hospital, campus, enterprise and residential buildings are instances of individual WMN domains subscribing to the Internet services from upstream SPs, shown as the Internet cloud in Fig. 1. Each WMN domain, or trust domain (to be used interchangeably) is managed by a domain administrator that serves as a trusted authority (TA), *i.e.*, the central server of a campus WMN. The TA and associated GWs are connected by high speed wired or wireless links, displayed as solid and bold dashed lines, respectively. TAs and GWs are assumed to be capable of handling computationally intensive tasks. In addition, they are assumed to be protected in private places and cannot be easily compromised due to their important roles in the WMN. The WMNs of interest here are those where the TA provides free Internet access but requires the clients (CLs) to be authorized and affiliated members generally for a long term, as the employees or students in the case of enterprise and hospital WMNs or campus WMNs. Such individual WMN domains can be building blocks of an even larger metropolitan WMN domain.

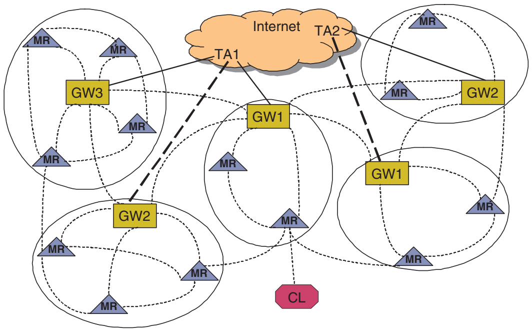

Fig. 1. Network Topology of A Typical WMN.

C. TRUST MODEL

1) TRUST RELATIONSHIP: In general, the TA is trusted within the WMN domain. There is no direct trust relationship between the CL and the GW/MR. We will use IBC for authentication and secure communications both at the backbone and during network access inside a trust domain (*i.e.*, intra-domain). We further assume the existence of pre-shared keys and secure communication channels between entities (TAs, GWs, MRs) at the backbone and will solely consider the authentication and key establishment during the network access of the CLs.

The CL presents its ID upon registration at the TA, which assigns a private key associated with the CL's ID. The CL selects a unique account number A computed by a randomly chosen secret number u_1 (cf. Section IV A 1)). The account number is stored with the CL's ID at the TA. The TA also assigns an ID/private key pair to each GW and MR in its trust domain before deployment. Advantages of this general trust relationship with the TA stem from the direct authentication of the CLs traveling amongst GWs/MRs in the same domain, which reduces network access latency and communication overhead that will be overwhelming in future WMNs due to the large subscriber population and their high mobility.

Due to the natural hierarchical architecture of the WMNs considered in this paper, we adopt the hierarchical ID-based signature scheme (HIDS) for inter-domain authentication that happens when a CL affiliated with the home TA visits neighboring foreign TAs. Note that the basic HIDS [33] is suitable when the level m of the signer in the hierarchical tree (HT) is close to the root at level 0, since the number of pairing operations and the size of the signature are determined by the signer's absolute location m. If m is relatively high (*i.e.*, the signer is located deep down the HT), the basic HIDS can be very inefficient in terms of the computation and communication overhead. In this case, Dual-HIDS [33] is more suitable if the signer and verifier share a common ancestor at level l below the root, since the number of pairing operations and the size of the signature are determined by the signer's relative location to the common ancestor $m - l$. For instance, the two TAs in Fig. 1 can be the domain administrators of neighboring campuses or hospitals directly managed by the state department of education (SDE), or the state department of health (SDH), etc. For simplicity, we use the basic HIDS for demonstrating the inter-domain authentication in this paper. Let the SDE (or SDH) be the root at level 0 in the HT of the campus (or hospital) WMN. All the TAs in the SDE's domain are at level 1 and all GWs, MRs and CLs in each TA's domain are at level 2. Note that in reality, the campus (or hospital) WMN may be part of the HT of a larger WMN (*i.e.*, the SDE or SDH is a child at level n below the root). However, as long as the signer's relative location to the common ancestor of the signer/verifier pair in the HT remains unchanged, the Dual-HIDS scheme can be employed instead.

In the WMN architecture in [12], we handled a similar inter-domain authentication issue with a different approach. When a CL roams to a foreign TA's domain (FTD) with a different master secret, we propose to get the foreign TA's domain parameters certified by a trusted third party (TTP). The domain parameter certificate (DPC) issued by the TTP is then included in the inter-domain authentication for verifying the authenticity of the domain parameters, which will later be utilized to verify the signature from the entities in FTD. Compared to that approach, the adopted HIDS scheme eliminates the requirement for the TTP and the DPCs. Furthermore, since we are concerned with the computation power of the CLs, using the level assignment (levels 0-2) mentioned in the example above, the CL need compute 4 pairings for verifying the signature from the AP (the MR or GW). In [12], the CL need also compute 4 pairings, 2 for DPC validation and 2 for verifying the signature from the AP if the efficient Hess's ID-based signature [34] is used. Thus, the adopted HIDS scheme does not compromise the computation efficiency while avoiding the TTP and DPCs. We argue that the computational complexity of HIDS for the WMN architecture considered here is acceptable since the CL is most frequently roaming within the home domain where the standard IBC is used.

2) TRUST DOMAIN INITIALIZATION: We apply the domain initialization of the hierarchical IBC [33]. Specifically, the root PKG (public key generator) at level 0 in the HT performs the following domain initialization algorithm when the network is bootstrapped, where P_0 is a generator of G_1.

1) Input security parameter $\xi \in Z^+$ into domain parameter generator $\mathcal{PG}$ and output the parameter tuple $(q, G_1, G_2, e, P_0, H_1)$.
2) Randomly select a domain master secret $s_0 \in Z_q^*$ and calculate the domain public key $\overline{P_{pub}} = s_0 P_0$.

The root PKG (*e.g.*, the SDE or SDH) publishes the domain parameters $(q, G_1, G_2, e, P_0, H_1, \overline{P_{pub}})$ and maintains s_0 confidential. Suppose a child CH_j is located at level j. The lower-level setup is performed by the parent as follows.

1) Compute $K_j = H_1(ID_1, ..., ID_j)$;
2) Compute CH_j's private keys $\psi_j = \psi_{j-1} + s_{j-1}K_j = \sum_{i=1}^{j} s_{i-1}K_i$, $\Gamma_j = \pi H_1(ID_j)$;
3) Distribute $QT = \{Q_l : 1 \leq l < j\}$ to CH_j, where $Q_l = s_l P_0$.

In the above private key assignment, $(ID_1, ..., ID_i)$ for $1 \leq i \leq j$ is the ID tuple of CH_j's ancestor at level i. ψ_j and Γ_j are the private keys generated by the parent's secret numbers $s_{j-1}, \pi \in Z_q^*$ and are to be used at the inter-domain and intra-domain authentication, respectively. For instance in Fig. 1, TA1 is the parent of all the entities in its domain which is located at level 1. The entities (GWs, MRs, CLs) are TA1's children at level 2. Similarly, the SDE or SDH (root PKG in our simple illustration) at level 0 is the parent of TA1. Note that due to the hardness of DLP, it is not possible to solve for s_{j-1} or π given any private key calculated from them with non-negligible probability.

IV. THE PROPOSED SECURITY ARCHITECTURE

A. TICKET-BASED SECURITY ARCHITECTURE

First, we restrict our discussion to within the home domain. The inter-domain protocols in our security architecture, which are executed when the CL roams outside its home domain, will be presented in A 5). The ticket-based anonymity scheme consists of ticket issuance, ticket deposit, fraud detection, and ticket revocation protocols. In what follows, we will describe these protocols in detail, together with the authentication, data integrity check, and confidential communications that may take place during the execution of these protocols.

1) TICKET ISSUANCE: In order to maintain the fairness among CLs and the security of the network against malicious attacks, the home TA may control the access of each CL by issuing tickets based on the non-conformed behavior history of the CL which reflects the TA's confidence about the CL to act properly. Ticket issuance occurs when the CL initially attempts to access the network or when all previously issued tickets are depleted. The CL need reveal its real ID to the TA in order to obtain a ticket since the TA has to ensure the authenticity of this CL. Moreover, the TA should be unable to link the ticket it issued to the CLs' real identities. Therefore, the CL employs some blinding techniques to transform the ticket to be unlinkable to any specific execution of the ticket generation algorithm, while maintaining the verifiability of the ticket. The ticket generation algorithm, which can be any restrictive partially blind signature scheme in the literature, takes input parameters including the CL's and TA's secret numbers, the common agreement c, and some public parameters, and generates a valid ticket $ticket = \{T_N, W, c, (U', V', X', \rho, \sigma_1', \sigma_2')\}$ at the output, where T_N is the unique serial number of the ticket which can be represented by the CL's account number A, $(U', V', X', \rho, \sigma_1', \sigma_2')$ is the signature on (T_N, W, c), W is necessary for verifying the validity of the signature in the ticket deposit protocol. Partially blind signatures alone allow the blind signature to carry explicit information on commonly agreed terms (*i.e.*, ticket value, expiry date, misbehavior, *etc.*) which remains publicly visible regardless of the blinding process. Restrictive blind signatures place restrictions on the CL's selection of messages being signed which contain encoded identity information (in T_N) instead of completely random numbers, allowing the TA to recover the CL's identity by computing A *if and only if* misbehavior is detected. As a result, the anonymity of an *honest* CL is unconditionally ensured. Exemplary restrictive partially blind signature schemes [31], [32] can be adopted as the ticket generation algorithm in our ticket issuance protocol.

The TA publishes the domain parameters to be used within its trust domain as $(q, G_1, G_2, e, P, P_1, P_2, H_1, H_2, H_3, P_{pub})$ using the standard IBC domain initialization, where (P, P_1, P_2) are random generators of G_1, and $P_{pub} = \pi P$ Since the scheme of [32] is selected for demonstration, G_1 here should be a Gap Diffie-Hellman (GDH) group [35] where the computational Diffie-Hellman problem (CDHP) [35] is assumed to be intractable. In addition, the TA chooses $r \in_R Z_q^*$ and $Q \in_R G_1$, and the CL chooses $\alpha, \beta, \gamma, \tau, \lambda, \mu, \rho \in_R Z_q$. Note that if the scheme of [31] is adopted, the TA publishes $(q, G_1, G_2, e, g, g_1, g_2, H, H_0, H_1)$, where G_1 should be a GDH in which the RCDHP (reversion CDHP) is assumed to be intractable (refer to [31] for detailed definitions). For simplicity, we will only demonstrate the following protocols based on the scheme of [32]. The application of the scheme in [31] to our protocols is straightforward following a similar procedure. The ticket issuance protocol is demonstrated as:

1) $CL \rightarrow\rightarrow TA$: ID_{CL}, m, t_1, $\mathcal{HMAC}_\kappa(m \parallel t_1)$;
2) $TA \rightarrow\rightarrow CL$: ID_{TA}, $X = e(m, \Gamma_{TA})$, $Y = e(P, Q)$, $Z = e(m, Q)$, $U = rH_1(ID_{TA})$, $V = rP$, t_2, $\mathcal{HMAC}_\kappa(X \parallel Y \parallel Z \parallel U \parallel V \parallel t_2)$;
3) $CL \rightarrow\rightarrow TA$: ID_{CL}, $B = \frac{1}{\lambda}H_2(m' \parallel U' \parallel V' \parallel R \parallel W \parallel X' \parallel Y' \parallel Z') + \mu$, t_3, $\mathcal{HMAC}_\kappa(B \parallel t_3)$;
4) $TA \rightarrow\rightarrow CL$: ID_{TA}, $\sigma_1 = Q + B\Gamma_{TA}$, $\sigma_2 = (r + B)\Gamma_{TA} + rH_1(c)$, t_4, $\mathcal{HMAC}_\kappa(\sigma_1 \parallel \sigma_2 \parallel t_4)$.

At the end, the CL checks if the following equalities hold: $e(P, \sigma_1) = y^B Y$ and $e(m, \sigma_1) = X^B Z$, where $y = e(P_{pub}, H_1(ID_{TA}))$. If the verification succeeds, the CL calculates $\sigma_1' = \gamma\sigma_1 + \tau H_1(ID_{TA})$, $\sigma_2' = \lambda\sigma_2$, $\rho = \gamma B$, and outputs the signature $(U', V', X', \rho, \sigma_1', \sigma_2')$ on (T_N, W, c), where $T_N = m'$. In Step 3) above, $m = u_1P_1 + u_2P_2 = A + u_2P_2 \neq 0$ and let $u_2 = 1$ here, $m' = \alpha m$, $U' = \lambda U + \lambda\mu H_1(ID_{TA}) - \beta H_1(c)$, $V' = \lambda V + \beta P_{pub}$, $R = e(m', H_1(ID_{TA}))$, $W = g_1^{v_1} g_2^{v_2}$ with $g_1 = e(P_1, H_1(ID_{TA}))$ and $g_2 = e(P_2, H_1(ID_{TA}))$, $X' = X^\alpha$, $Y' = Y^\gamma g^\tau$ with $g = e(P, H_1(ID_{TA}))$, $Z' = Z^{\alpha\gamma} R^\tau$. In the above protocol, the TA and the CL can locally derive a symmetric key $\kappa = e(\Gamma_{TA}, H_1(ID_{CL}))$, and $\kappa = e(H_1(ID_{TA}), \Gamma_{CL})$, respectively, assuming that ID_{TA} is known to all entities in the TA's domain. A timestamp t_i is included in each message exchanged to prevent the message replay attack [3]. Note that some pairings such as the those for g_1, g_2 and g in the above procedure can be pre-computed once and stored for all future use, thus alleviating the computation burden of the CL.

A design issue to be pointed out is the commonly agreed information c negotiated at the beginning of the ticket generation algorithm. We define c as $(val, exp, misb)$ where val, exp and $misb$ denote the ticket value, expiry date/time, and the CL's misbehavior level, respectively. The ticket value confines the total amount of traffic that the CL is allowed to generate and receive before the expiry date of the ticket. Tickets bear different values. The CL's $misb$ field conveys information on the misbehavior history of the CL in the network. This information is summarized at the TA by performing the fraud detection based on the ticket records reported by GWs which have served this CL. By placing the misbehavior information in c, the TA successfully informs GWs about the CL's past misbehavior when the ticket is deposited. The incorporation of the $misb$ field has several merits. One possible merit would be to punish CLs with misbehavior history by higher network access latency. The GW may intend to serve the well-behaved CLs immediately upon receiving the ticket and reports the ticket record to the TA at a later time. If the CL appears to have misbehaved previously and thus may cast a threat on network operations, the GW will first report the ticket record to the TA and will serve the CL only if the TA returns positive feedback (*i.e.*, the TA performs ticket fraud detection to check if this ticket has been deposited before). Since we assume an offline TA in our scheme, the network access delay cannot be bounded and depends on the work load of the TA.

2) TICKET DEPOSIT: After obtaining a valid ticket, the CL may deposit it anytime the network service is desired before the ticket expires, using the ticket deposit protocol shown below. Our scheme restricts the ticket to be deposited only once at the first encountered GW which provides network access services to the CL according to val before exp.

1) $CL \rightarrow\rightarrow GW$: PS_{CL}, m', W, c, $\sigma = (U', V', X', \rho, \sigma_1', \sigma_2')$, t_5, $\mathcal{SIG}_{\widetilde{\Gamma_{CL}}}(m' \parallel W \parallel c \parallel \sigma \parallel t_5)$;
2) $GW \rightarrow\rightarrow CL$: ID_{GW}, $d = H_3(R \parallel W \parallel ID_{GW} \parallel T)$, t_6, $\mathcal{HMAC}_{\kappa'}(d \parallel t_6)$;
3) $CL \rightarrow\rightarrow GW$: PS_{CL}, $r_1 = d(u_1\alpha)+v_1$, $r_2 = d\alpha+v_2$, t_7, $\mathcal{HMAC}_{\kappa'}(r_1 \parallel r_2 \parallel t_7)$;
4) $GW \rightarrow\rightarrow CL$: ID_{GW}, $misb$, exp, t_8, $\mathcal{SIG}_{\Gamma_{GW}}(PS_{CL} \parallel ID_{GW} \parallel misb \parallel exp \parallel t_8)$;

At the end, the GW checks if the equality $g_1^{r_1} g_2^{r_2} = R^d W$ holds. At the end of Step 1), the GW will perform $\mathcal{VER}(\sigma)$ before Steps 2) and 3) can be proceeded, and R can be derived as $R = e(m', H_1(ID_{TA}))$ from the received information. T is the date/time the ticket is deposited. A symmetric key κ' can be derived locally by the GW and the CL as $\kappa' = e(\Gamma_{GW}, PS_{CL})$, and $\kappa' = e(H_1(ID_{GW}), \widetilde{\Gamma_{CL}})$, respectively, after learning each other's ID (or pseudonym). The generation of the pseudonym will be discussed in IV B.

The ticket is deemed valid if both the signature verification and the above equality check succeed. The deposit GW (DGW), where the ticket is initially deposited will then generate a signature on the CL's pseudonym, the DGW's ID, and the associated $misb$ and exp values extracted from c. The signature is required to be present in order for other APs in the trust domain to determine whether and where to forward the CL's access requests, if the deposited ticket will be further used from other APs (excluding the DGW). This is the reason that the CL is not allowed to change its pseudonym while still using a deposited ticket to which the pseudonym is associated, since the DGW will refuse to offer access services to the CL if the presented pseudonym mismatches the one recorded with the ticket. As a result, the ticket value need be set to a relatively small quantity in order to allow frequent update of the pseudonym if the CL has high requirement on its anonymity [10], [18]. It will not place extra signaling overhead into the system since the TA can grant a batch of small-valued tickets during one single ticket issuance protocol. Due to the limited ticket value, the CL is expected to have minimal mobility during the usage of the deposited ticket. However, there are also cases where the CL moves to other GWs after the ticket is deposited. To address this issue, possible decision making functionalities may be incorporated into GWs. For instance, if the CL temporarily moves to a new GW in the DGW's vicinity, the new GW can merely forward all the traffic of this CL to the DGW which then serves the CL based on the deposited ticket. If the CL permanently moves to a new GW, the new GW may request the DGW to transfer the ticket record so that the new GW can directly serve the CL. We do not intend to further address this issue. Instead, a simple and efficient solution can be employed which is to abandon the usage of the remaining ticket and deposits a new one at the new GW since the ticket value is generally not very large. This solution is also effective in the case where the ongoing service is disrupted due to channel impairments, route failure, or mobility. Adopting this solution, Step 4) in the above procedure can be omitted.

The DGW then creates a record for the deposited ticket as: $record = (ticket, r_1, r_2, T, rem, log)$, where rem and log denote the remaining value of the ticket and the logged data of the CL's non-conformed behavior, respectively. When the CL uses the ticket to gain network access, the DGW initiates a traffic counter and decreases it based on the amount of traffic the CL has injected and received. The remaining ticket value rem defines the amount of network access service the CL will be offered before the ticket is depleted. We do not constrain the number of tickets the CL can request or the request frequency in the proposed scheme, rendering the opportunity for CLs to inject a large amount of traffic or even to launch DoS (Denial of Service) attack, by gaining a considerable number of tickets in hand. Therefore, the log field is created to record such non-conformed behavior so that when receiving the ticket record from the DGW, the TA is able to apply certain constraints on the CL's future requests, if any, based on the logged data in log. For instance, the TA may decrease the value of the issued tickets or reduce the frequency of approving the CL's ticket requests. Note that the non-conformed behavior is different from the misbehavior which solely refers to ticket-reuse and multiple-deposit. The ticket record will be deleted from the DGW's database once the ticket expires (by checking c) and the most recent record (excluding rem) has been reported to the TA. Note that the DGW will maintain the record for the depleted tickets that have not expired in order to prevent the CL from re-depositing such tickets at this DGW. For CLs with satisfactory $misb$ values, the ticket record is sent to the TA periodically, while it is sent to the TA before any network access service can be offered for CLs with inferior $misb$ values, as mentioned before. These values are obtained and updated by fraud detection to be discussed shortly.

3) FRAUD DETECTION: Fraud is used interchangeably with misbehavior in this paper, which is essentially an insider attack. Ticket-reuse generally results from the CL's inability to obtain tickets from the TA when network access is desired, primarily due to the CL's non-conformed behavior which causes the TA to constrain its ticket requests. Multiple-deposit can also be termed CL coalition, which is beneficial when the coalescing CLs are unauthorized users or CLs with non-conformed behavior that have difficulty in acquiring tickets from the TA. Note however that, since a CL is able to obtain multiple tickets in one ticket issuance protocol and self-generate multiple pseudonyms (cf. IV B), it can distribute these pseudonym/ticket pairs to other CLs without being traced as long as each ticket is deposited only once. One possible solution to this flaw is to specify the non-overlapping active period of a ticket instead of merely the expiry date/time, such that each time only one ticket can be valid. This approach in general requires synchronization. Another solution is to adopt the tamper-proof secure module (SM) so that a CL cannot disclose its secrets to other CLs since the content of the SM is assumed to be expensive and impractical to access or manipulate. This approach will eliminate the committing of the multiple-deposit fraud but requires the deployment of the SMs. In the following discussion, we will still consider multiple-deposit as a possible type of fraud (*e.g.*, in case SMs are unavailable).

These two types of fraud share a common feature, that is, a same ticket (depleted or valid) is deposited more than once which violates our one-time deposit rule. This is where the restrictiveness of the blind signature algorithm takes effect on revealing the real identity of the misbehaving CL. Specifically, when the TA detects duplicate deposits using the ticket records reported by GWs, the TA will have the view of at least two different challenges from GWs and two corresponding sets of responses from the same CL. By solving the equation sets below based on these challenges and responses, the TA is able to obtain the identity information encoded in the message and hence the real identity of the misbehaving CL. The fraud detection protocol is shown as:
$GW \rightarrow TA$: ID_{GW}, m', W, c, $\sigma = (U', V', X', \rho, \sigma'_1, \sigma'_2)$, r_1, r_2, T, t_9, $\mathcal{HMAC}_{\kappa''}(m' \parallel W \parallel c \parallel \sigma \parallel r_1 \parallel r_2 \parallel T \parallel t_9)$, where κ'' is the pre-shared symmetric key between the GW and the TA, which we have assumed for the WMN backbone. At the end, the TA performs $\mathcal{VER}(\sigma)$. If the signature can be successfully verified, the TA checks if m' (or the ticket serial number T_N) has been stored. If m' is not stored, the TA will store the following information: m', c, T, r_1, r_2 for future fraud detection, and log for updating the CL's non-conformed behavior data. If m' has been stored, the TA will first compute the challenge $d = H_3(R \parallel W \parallel ID_{GW} \parallel T)$ and will accuse the GW if d is the same as the stored one. If d is different, the TA can conclude that misbehavior has occurred and will reveal the identity information by constructing the following two sets of equations from two different views of the ticket records received from GWs:

$$r_1 = d(u_1\alpha) + v_1, r_2 = d\alpha + v_2 \quad (1)$$

$$r'_1 = d'(u_1\alpha) + v_1, r'_2 = d'\alpha + v_2 \quad (2)$$

The TA can solve for $u_1 = \frac{r_1 - r'_1}{r_2 - r'_2}$ and obtain the account number $A = u_1 P_1$ to reveal the associated identity ID_{CL}.

By far, we have presented the techniques in our anonymity scheme to resolve the conflicts between anonymity and traceability. As long as the CL is a well-behaved user in this network, its anonymity can be fully guaranteed. This is achieved by the blinding process of the ticket issuance protocol which breaks the linkage between the ticket and the identity, *i.e.*, the TA knows the CL's real ID but does not know which ticket/pseudonym pairs belong to this CL, while the GW knows the linkage between the ticket and the pseudonym but learns no information on the real identity of the owner of these pairs. On the other hand, if the CL misbehaves (*i.e.*, fraud occurs), the CL's anonymity can no longer be guaranteed since the TA may tend to identify and punish this CL possibly by revoking the CL's network access privilege, utilizing the traceability property offered by the proposed anonymity scheme. In addition, our system enables authentication at the APs and conforms to the access control security requirement that is not satisfied in [17] where no authentication of the CL is performed at the AP in the controlled connection protocol. Note that the real ID of a CL is learned by the home TA and the AP only during ticket issuance. Since a batch of tickets can be issued each time and the CL may still hold unused tickets, the deposit procedure of a specific ticket cannot be deduced by estimating the timing relationship between the issuance and the deposit. Although the CL's ID cannot be hidden from the home TA due to the requirement for issuing tickets, it can be hidden from the AP by additional mechanisms. In this case, the CL can deposit a ticket (using the ticket deposit protocol) merely for obtaining new tickets and send the ticket request in ciphertext to the home TA. It is acceptable that the activity of the CL with this particular ticket (*i.e.*, to request new tickets) may be revealed by the collusion of the home TA and the DGW, since this activity is not necessary to be concealed.

4) TICKET REVOCATION: Ticket revocation is necessary when a CL is compromised and thus all its secrets are disclosed to the adversary. In our system, the adversary is motivated by gaining network services using tickets once the ticket-associated secrets are obtained from the compromised CLs. Therefore, the compromised CL need be able to revoke the ticket and prevent the adversary from acquiring benefits. Since the compromised CL and the adversary are the only two parties that know the CL's secrets, a valid revocation request must be sent by the compromised CL for genuine revocation purpose. The ticket revocation protocol consists of two cases:

1) Revocation of new tickets: the CL may store a number of unused tickets, as mentioned previously. When revoking these tickets that have not been deposited, CL sends PS_{CL}, T_N, t_{10}, $\mathcal{SIG}_{\widetilde{\Gamma_{CL}}}(T_N \parallel t_{10})$ in the revocation request to any encountered GW. This GW authenticates the CL using PS_{CL} and records the ticket serial number T_N as revoked.
2) Revocation of deposited tickets: the CL simply sends PS_{CL}, ID_{DGW}, t_{11}, $\mathcal{SIG}_{\widetilde{\Gamma_{CL}}}(ID_{DGW} \parallel t_{11})$ in the revocation request to the DGW. The DGW authenticates the CL and marks the associated ticket revoked.

When GWs have records in the revocation database, they immediately report the revocations to the associated TA which will update and distribute the revocation list for all GWs in the trust domain to reference.

5) ACCESSING THE NETWORK FROM FOREIGN DOMAINS: The access services the visiting (foreign) trust domain provides in the ticket-based security architecture can take place in two ways including:

- A foreign mesh router $\overline{MR}$ (or any AP) forwards the CL's new ticket request to the home domain when there is no available ticket for accessing the network from the foreign domain:
  1) $CL \rightarrow\rightarrow \overline{MR}$: PST_{CL}, aP_0, t_{12}, $\mathcal{HIDS}_{\psi_{CL},s_{CL}}(H_1'(PST_{CL} \parallel aP_0 \parallel t_{12}))$;
  2) $\overline{MR} \rightarrow CL$: $IDT_{\overline{MR}}$, bP_0, t_{13}, $\mathcal{HIDS}_{\psi_{\overline{MR}},s_{\overline{MR}}}(H_1'(IDT_{\overline{MR}} \parallel bP_0 \parallel t_{13}))$;
  3) $CL \rightarrow\rightarrow \overline{MR}$: PST_{CL}, PS_{CL}, $\mathcal{SKE}_\kappa(ID_{CL} \parallel m)$, t_{14}, $\mathcal{HMAC}_{\bar{\kappa}}(PS_{CL} \parallel \mathcal{SKE} \parallel t_{14})$.
- $\overline{MR}$ (or any AP) forwards the CL's ticket deposit request to the home domain when the CL owns available new tickets issued by the home TA. The first two steps of the procedure are exactly the same as above. The last step in this case will be:
  $CL \rightarrow\rightarrow \overline{MR}$: PST_{CL}, PS_{CL}, $ticket$, t_{15}, $\mathcal{HMAC}_{\bar{\kappa}}(PS_{CL} \parallel ticket \parallel t_{15})$.

At the end, $\overline{MR}$ will forward the network access request consisting of $(PS_{CL}, \mathcal{SKE}_\kappa(ID_{CL} \parallel m))$ with κ the symmetric key between the CL and its home TA, or $(PS_{CL}, ticket)$, to an AP (a GW or MR) in the CL's home domain, if $\mathcal{HVER}(\mathcal{HIDS} \parallel QT)$ outputs "accept" in Steps 1) and 2). The symmetric key between the CL and $\overline{MR}$ is $\bar{\kappa} = abP_0$, where $a, b \in_R Z_q^*$ and P_0 is the public domain parameter of the root PKG (cf. Section III C).

Notice that the above triangular traffic forwarding via the home domain can be cumbersome if the CL will stay at a foreign domain for a long term (*e.g.*, not temporarily visiting). It is recommended that the CL registers with the foreign TA to become an affiliated user of the foreign domain. Consequently, all the network access related operations including ticket issuance, deposit, revocation and fraud detection will follow as in the home domain, which will greatly reduce the communication overhead in the system.

B. PSEUDONYM GENERATION AND REVOCATION

The use of pseudonyms has been shown in the ticket-based protocols. This section copes with the pseudonym generation technique and the related revocation issue. The pseudonym is used to replace the real ID in the authentication which is necessary for both anonymous network access and location privacy. In the intra-domain authentication in our system, the CL generates its own pseudonym by selecting a secret number $\varpi \in_R Z_q^*$ and computing the pseudonym $PS_{CL} = \varpi H_1(ID_{CL})$. The corresponding private key can be derived as $\widetilde{\Gamma_{CL}} = \varpi\Gamma_{CL} = \varpi\pi H_1(ID_{CL}) = \pi \cdot PS_{CL}$, in a similar way to that of [36]. Compared to [10], [12], [16] where a batch of pseudonyms are assigned to each CL by the TA, the self-generation method greatly reduces the update overhead at the CL and the signaling overhead in the system. Moreover, the CL is able to frequently update its pseudonyms (with tickets) to enhance anonymity by using this inexpensive method.

In the inter-domain authentication in our system, suppose a client CL_j residing at level j is requesting network access from a foreign mesh router $\overline{MR}$ in a visiting trust domain. After obtaining the private key ψ_j associated with the ID tuple $IDT_j = (ID_1, ..., ID_j)$ as $\psi_j = \psi_{j-1} + s_{j-1}H_1(IDT_j)$ from the parent (*i.e.*, the home TA), we derive the self-generated pseudonym tuples $\{PST_i : 1 \leq i \leq j\}$ for CL_j as follows: CL_j selects a random secret $\varpi \in Z_q^*$ and computes the pseudonym tuples $PST_i = \varpi K_i = \varpi H_1(IDT_i)$ $(1 \leq i \leq j)$. The associated private key can be computed as $\widetilde{\psi_j} = \varpi\psi_j = \varpi\sum_{i=1}^{j} s_{i-1}K_i = \sum_{i=1}^{j} s_{i-1}\varpi K_i = \sum_{i=1}^{j} s_{i-1}\varpi H_1(IDT_i) = \sum_{i=1}^{j} s_{i-1} \cdot PST_i$. Substitute $PST_j/\widetilde{\psi_j}$ for $H_1(IDT_j)/\psi_j$ in the HIDS scheme [33], the signing and verification can be correctly performed.

As a final note on the self-generation algorithm, it would render the pseudonym revocation impossible by using the pseudonym alone. The reason is that any adversary who has compromised a CL can generate valid pseudonym/key pairs that are only known to the adversary by running the self-generation algorithm. However, this pseudonym generation technique is appropriate in our system because the pseudonym revocation can be realized via revoking the associated ticket since the pseudonym is active only when its associated ticket is actively in use (deposited and not depleted). Therefore, the revocation process described in *A. 4)* for ticket revocation automatically revokes ticket-binding pseudonyms. If we employ the pseudonym assignment as in [10], [12], [16], the TA will be able to derive the real identity corresponding to the assigned pseudonyms, which destroys the anonymity property for honest CLs.

V. SECURITY ANALYSIS

In this section, we analyze the security requirements our system can achieve as follows.

Fundamental security objectives-It is trivial to show that our security architecture satisfies the security requirements for authentication, data integrity and confidentiality, which follows directly from the employment of the standard cryptographic primitives, namely, digital signature, message authentication code, and encryption, in our system. We are only left with the proof of non-repudiation in this category. A fraud can be repudiated only if the CL can provide a different representation (u_1, u_2) it knows of m from what is derived by the TA. If the CL has misbehaved, the representation it knows will be the same as the one derived by the TA which ensures non-repudiation.

Anonymity-First of all, it can be easily shown that a GW cannot link a legitimate CL's network access activities to the CL's real identity. Due to the use of pseudonyms in authentication which reveals no information on the real ID, the GW learns nothing about the identity of the CL requesting network access. Since the pseudonym is generated by the CL using a secret number, solving for the real identity from the pseudonym is equivalent to solving the DLP. Furthermore, the CL's DGW cannot deduce the CL's ID from the deposited ticket which has been blinded by the CL and does not reveal any identification information unless misbehavior occurs. Next, we will show that the CL's home TA cannot perform such linking either which follows directly from Theorem 3 of [32] that the restrictive partially blind signature scheme used as a building block for our security architecture is partially blind. Specifically, as in [32], any view of the ticket issuance protocol $(U, V, X, Y, Z, B, \sigma_1, \sigma_2, m)$ is unlinkable to any valid signature $(U', V', X', \rho, \sigma'_1, \sigma'_2, m')$ because it is proven in [32] that the blinding factors $(\alpha, \gamma, \tau, \lambda, \mu, \beta)$ always exist which maps $(U, V, X, Y, Z, B, \sigma_1, \sigma_2, m)$ to $(U', V', X', \rho, \sigma'_1, \sigma'_2, m')$. Therefore, even an infinitely powerful $\mathcal{S}^*$ wins the game with probability $\frac{1}{2}$ (see [32]) which is equivalent to random guessing. Finally, we will show that even the collusion of the home TA and the DGW cannot carry out the linking. It is obvious that by collusion, the TA can learn no more from the GW than the CL's pseudonym used in association with a deposited ticket. The hardness of deducing a real identity from a pseudonym has been mentioned above. On the other hand, the GW can learn the following from the TA: the private key, the account number, and the view of the ticket issuance protocol $(U, V, X, Y, Z, B, \sigma_1, \sigma_2, m)$ of a randomly chosen target ID. Thus, the maximal amount of information the TA and GW can exploit by collusion is 1) from the GW: a ticket $m', W, c, (U', V', X', \rho, \sigma'_1, \sigma'_2)$ deposited by some CL with an unknown-yet-authentic pseudonym for network access; 2) from the TA: a randomly chosen target identity, its associated private key, account number, and the view $(U, V, X, Y, Z, B, \sigma_1, \sigma_2, m)$ of the ticket issuance protocol. It is straightforward that because of the partial blindness of the adopted signature scheme and the hardness of solving DLP as shown above, the information pieces in 1) and 2) are unlinkable other than random guessing.

Traceability (conditional anonymity)-According to its definition, this requirement is two-fold: 1) Anonymity for honest CLs is unconditional, which can be proven following Propositions 10 and 13 of [27]; 2) A misbehaving CL is traceable where the identity can be revealed. The proof of 2) follows from Theorem 2 of [32] that the adopted restrictive partially blind signature scheme in our security architecture achieves restrictiveness. In other words, 2) says that the CL can only obtain signatures on messages of which the CL knows a representation for which the structure in the representation (where the identity information is encoded) remains, which can be proven by using Proposition 12 of [27] and two extra requirements on the representations the CL knows of m and m' (see [27] for detailed description of the two requirements).

Framing resistance-If the CL is honest, with overwhelming probability, the representation (u_1, u_2) it knows is different from that the malicious TA falsely generated. Since the CL could not have come up with this representation by itself, it proves that the TA attempts to frame the CL. Therefore, innocent CLs can exculpate themselves to prevent malicious TAs from revoking their network access privilege.

Unforgeability-The proof of unforgeability (formally defined in [32]) is essentially the proof of Theorem 4 of [32] that the adopted restrictive partially blind signature scheme is existential unforgeable against adaptively chosen message and ID attacks under the assumption of the intractability of CDHP in G_1 and the random oracle.

We conclude that: *The proposed security architecture satisfies the security requirements for anonymity, traceability, framing-resistance, and unforgeability, in addition to the fundamental objectives including authentication, data integrity, confidentiality and non-repudiation, under the assumption that CDHP in G_1 is hard and the random oracle.*

Due to the space limitation, the overhead analysis will be omitted here and details will be presented elsewhere.

VI. Security Enhancements

In addressing privacy and anonymity on the Internet, Dingledine [37] argues that cryptography alone will not hide the existence of confidential communication relationships and implemented an anonymous communication overlay network, Tor [22], based on the anonymous routing protocol, *i.e.*, the onion routing [21]. In addressing the privacy preserving issue in vehicular ad hoc networks (VANETs) where the vehicles enjoy various VANET applications, Raya and Hubaux [10] claim that all vehicle identifiers, in particular the MAC and IP addresses, must change over time, in addition to the frequent update of the anonymous keys (pseudonyms). Analogously, the proposed ticket-based anonymity system relies on effective anonymous routing protocols to construct anonymous communication paths and guarantee anonymity for the CLs across the entire WMN system. For instance, if the network ID (*i.e.*, IP address, MAC address) of a CL's device is fixed and exposed in packet forwarding, the anonymity property of the proposed system will be undermined. By incorporating anonymous routing protocols [19], [20] into our system, the real network ID, if used in communications, will be effectively concealed in traffic forwarding involving the CL, which renders it difficult for the attacker to trace the packet forwarding path and discover the confidential relationship of the communicating parties.

Another possible enhancement is to incorporate peer-to-peer cooperation. In the WMNs considered here, the uplink from the CL to the MR may rely on multi-hop communications. Peer CLs act as relaying nodes to forward each other's traffic to the MR, which forms a P2P network. The notorious problem common in P2P communication systems is the free-riding, where some peers take advantage of the system by providing little or no service to other peers or by leaving the system immediately after the service needs are satisfied. Peer cooperation is thus the fundamental requirement for P2P systems to operate properly. Since peers are assumed to be selfish, incentive mechanisms become essential to promote peer cooperation in terms of both cooperativeness and availability [15]. Typical incentive mechanisms for promoting cooperativeness include reputation-based [38], [39] and payment-based [40] approaches. In the reputation-based systems, peers are punished or rewarded based on the observed behavior. However, low availability remains an unobservable behavior [15] in such systems which hinders the feasibility of the reputation-based mechanism in improving peer availability. By contrast, the payment-based approach provides sufficient incentives for enhancing both cooperativeness and availability, and thus is ideal to be employed in multi-hop uplink communications among peer CLs in our WMN system.

VII. Conclusion

In this paper, we propose a security architecture mainly consisting of the ticket-based anonymity scheme, which resolves the conflicting security requirements of unconditional anonymity for honest users and the traceability of misbehaving users, and can be deemed as an application-layer protocol. By utilizing this anonymity scheme, the self-generated pseudonyms, and the hierarchical IBC, the proposed scheme is demonstrated to achieve desired security objectives.

Acknowledgment

This work was supported in part by the U.S. National Science Foundation under grants CNS-0721744, CNS-0716450 and CNS-0626881. The work of Fang was also supported in part by the National Science Council (NSC), R.O.C., under the NSC Visiting Professorship with contract number NSC-96-2811-E-002-010.

References

[1] S. Brands, "Untraceable off-line cash in wallets with observers," *in Proc. CRYPTO'93, 13th Annual Int'l Cryptology Conf. on Advances in Cyptology*, pp. 302–318, Aug. 1993.

[2] K. Wei, Y. R. Chen, A. J. Smith, and B. Vo, "Whopay: A scalable and anonymous payment system for peer-to-peer environments," *Proc. IEEE Intl. Conf. on Distributed Computing Systems, ICDCS*, July 2006.

[3] A. Menezes, P. V. Oorschot, and S. Vanston, *Handbook of Applied Cryptography*, Boca Raton, CRC Press, 1996.

[4] European Telecommunications Standards Institute (ETSI), "GSM 2.09: Security Aspects.," June 1993.

[5] P. Kyasanur and N. H. Vaidya, "Selfish MAC layer misbehavior in wireless networks," *IEEE Trans. Mobile Computing*, vol. 4, no. 5, pp. 502–516, Sept. 2005.

[6] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Comm. of the ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[7] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Trans. Sensor Networks*, vol. 2, no. 4, pp. 500–528, Nov. 2006.

[8] W. Lou and Y. Fang, *A Survey on Wireless Security in Mobile Ad Hoc Networks: Challenges and Possible Solutions*, edited by X. Chen, X. Huang and D.-Z. Du, Kluwer Academic Publishers/Springer, 2004.

[9] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Network Magazine*, vol. 13, no. 6, pp. 24–30, Dec. 1999.

[10] M. Raya and J-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks*, vol. 15, no. 1, pp. 39–68, 2007.

[11] N. B. Salem and J-P. Hubaux, "Securing wireless mesh networks," *IEEE Wireless Communications*, vol. 13, no. 2, Apr. 2006.

[12] Y. Zhang and Y. Fang, "ARSA: An attack-resilient security architecture for multihop wireless mesh networks," *IEEE J. Select. Areas Communications*, vol. 24, no. 10, pp. 1916–1928, Oct. 2006.

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

[14] D. Chaum, A. Fiat, and M. Naor, *Untraceable electronic cash*, in Proc. on Advances in Cryptology (CRYPTO'88), 2002.

[15] D. Figueiredo, J. Shapiro, and D. Towsley, "Incentives to promote availability in peer-to-peer anonymity systems," *in Proc. IEEE Int'l Conf. on Network Protocols, ICNP*, pp. 110–121, Nov. 2005.

[16] G. Ateniese, A. Herzberg, H. Krawczyk, and G. Tsudik, "Untraceable mobility or how to travel incognito," *Comput. Netw.*, vol. 31, no. 8, pp. 871884, Apr. 1999.

[17] Q. He, D. Wu, and P. Khosla, "Quest for personal control over mobile location privacy," *IEEE Communications Magazine*, vol. 42, no. 5, pp. 130–136, May 2004.

[18] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Computing*, vol. 2, pp. 46–55, 2003.

[19] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "MASK: Anonymous on-demand routing in mobile ad hoc networks," *IEEE Trans. Wireless Communications*, vol. 5, no. 9, pp. 2376–2385, Sept. 2006.

[20] S. Seys and B. Preneel, "ARM: Anonymous routing protocol for mobile ad hoc networks," *Proc. 20th Int'l Conf. on Advanced Information Networking and Applications, AINA*, pp. 133–137, Apr. 2006.

[21] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Anonymous connections and onion routing," *IEEE J. Select. Areas Communications*, vol. 16, no. 4, pp. 482494, May 1998.

[22] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," *in Proc. of The 13th USENIX Security Symposium*, p. 303320, Aug. 2004.

[23] D. Chaum, *Blind signatures for untraceable payments*, Advances in Cryptology - Crypto '82, pp. 199-203, Springer-Verlag, 1982.

[24] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," *IEEE Trans. Dependable and Secure Computing*, vol. 3, no. 4, pp. 386–399, Oct. 2006.

[25] D. Boneh and M. Franklin, *Identity-based encryption from the weil pairings*, Advances in Cryptology-Asiacrypt 2001, LNCS 2248, pp. 514-532, Springer-Verlag, 2001.

[26] A. Juels, M. Luby, and R. Ostrovsky, *Security of blind digital signatures*, Advances in Cryptology - CRYPTO '97, LNCS 1294, pp. 150-164, Springer-Verlag, 1997.

[27] S. Brands, *An efficient off-line electronic cash system based on the representation problem*, CWI Technical Report CS-R9323, 1993.

[28] M. Abe and T. Okamoto, *Provably secure partially blind signatures*, Advances in Cryptology - Crypto 2000, LNCS 1880, pp. 271-286, Springer-Verlag, 2000.

[29] S. M. Chow, C. K. Hui, S. M. Yiu, and K. P. Chow, *Two improved partially blind signature schemes from bilinear pairings*, ACISP 2005, LNCS 3574, pp. 316-328, Springer-Verlag, 2005.

[30] G. Maitland and C. Boyd, *A provably secure restrictive partially blind signature scheme*, LNCS 2274, pp. 99-114, Springer-Verlag, 2002.

[31] X. Chen, F. Zhang, Y. Mu, and W. Susilo, "Efficient provably secure restrictive partially blind signatures from bilinear pairings," *Proc. 10th Conf. on Financial Cryptography and Data Security, FC 2006*, pp. 251–265, Feb. 2006.

[32] X. Chen, F. Zhang, and S. Liu, "ID-based restrictive partially blind signatures and applications," *Journal of Systems and Software*, vol. 80, no. 2, pp. 164–171, Feb. 2007.

[33] C. Gentry and A. Silverberg, "Hierarchical id-based cryptography," *Proc. ASIACRYPT*, pp. 548–556, Dec. 2002.

[34] F. Hess, *Efficient identity-based signature schemes based on pairings*, SAC 2002, LNCS 2595, pp. 310-324, Springer-Verlag, 2002.

[35] R. Dutta, R. Barua, and P. Sarkar, *Pairing-based cryptography: a survey*, Cryptology ePrint Archive, Report 2004/064, available at http://eprint.iacr.org/2004/064.pdf, 2004.

[36] S. M. M. Rahman, A. Inomata, T. Okamoto, M. Mambo, and E. Okamoto, "Anonymous secure communication in wireless mobile ad-hoc networks," *Proc. 1st Intl. Conf. on Ubiquitous Convergence Technology*, pp. 131–140, Dec. 2006.

[37] R. Dingledine, "Tor: An anonymous internet communication system," *Workshop on Vanishing Anonymity, The 15th Conf. on Computers, Freedom, and Privacy*, Apr. 2005.

[38] S. Buchegger and J. L. Boudec, "The effect of rumor spreading in reputation systems for mobile ad-hoc networks," *in Proc. WiOpt'03*, Mar. 2003.

[39] Y. Zhang and Y. Fang, "A fine-grained reputation system for reliable service selection in peer-to-peer networks," *To Appear in IEEE Transactions on Parallel and Distributed Systems*.

[40] S. Zhong, J. Chen, and Y. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad hoc networks," *IEEE INFOCOM*, vol. 3, pp. 1987–1997, Apr. 2003.