An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks

Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang, *Fellow*, *IEEE*

Abstract—Vehicular ad hoc network (VANET) can offer various services and benefits to users and thus deserves deployment effort. Attacking and misusing such network could cause destructive consequences. It is therefore necessary to integrate security requirements into the design of VANETs and defend VANET systems against misbehavior, in order to ensure correct and smooth operations of the network. In this paper, we propose a security system for VANETs to achieve privacy desired by vehicles and traceability required by law enforcement authorities, in addition to satisfying fundamental security requirements including authentication, nonrepudiation, message integrity, and confidentiality. Moreover, we propose a privacy-preserving defense technique for network authorities to handle misbehavior in VANET access, considering the challenge that privacy provides avenue for misbehavior. The proposed system employs an identity-based cryptosystem where certificates are not needed for authentication. We show the fulfillment and feasibility of our system with respect to the security goals and efficiency.

Index Terms—Privacy, traceability, pseudonym, misbehavior, revocation, identity-based cryptography, vehicular ad hoc network.

1 Introduction

Vehicular ad hoc networks (VANETs) are receiving increasing attentions from academia and deployment efforts from industry, due to the various applications and potential tremendous benefits they offer for future VANET users. Safety information exchange enables life-critical applications, such as the alerting functionality during intersection traversing and lane merging, and thus, plays a key role in VANET applications [1], [2], [3], [4], [5]. Value-added services can enhance drivers' traveling experience by providing convenient Internet access, navigation, toll payment services, etc. [1], [3], [4], [5]. Other applications are also possible including different warning messages for congestion avoidance, detour notification, road conditions (e.g., slippery), etc., and alarm signals disseminated by emergency vehicles (e.g., ambulance) for road clearance [1], [2], [3], [5], [6]. The attractive features of VANETs inevitably incur higher risks if such networks do not take security into account prior to deployment. For instance, if the safety messages are modified, discarded, or delayed either intentionally or due to hardware malfunctioning, serious consequences such as injuries and even deaths may occur. This necessitates and urges the development of a functional, reliable, and efficient security architecture before all other implementation aspects of VANETs.

Fundamentally, VANET security design should guarantee authentication, nonrepudiation, integrity, and in some specific application scenarios, confidentiality, to protect the network against attackers. Besides the fundamental security requirements, sensitive information such as identity and location privacy should be preserved from the vehicle owner's perspective, against unlawful tracing and user profiling, since otherwise it is difficult to attract vehicles to join the network. On the contrary, traceability is required where the identity information need be revealed by law enforcement authorities for liability issues, once accidents or crimes occur. In addition, privilege revocation is required by network authorities (e.g., network administrator) once misbehavior is detected during network access. It is less difficult to prevent misbehavior of unauthorized users (i.e., outsiders) since legitimate users and roadside units (RSUs) can simply disregard communication requests from outsiders by means of authentication. Nevertheless, misbehavior of legitimate users of VANETs (i.e., insiders) is more difficult and complex to prevent, the reason being that insiders possess credentials issued by the authority to perform authentication with peer vehicles or RSUs who can be easily tricked into trusting the insiders. Consequently, the insiders' misbehavior will have much larger impact on the network and will be the focus of this paper. Our proposed system in this paper and many recent proposals on VANET security [3], [7], [8], [9] provide the option of using anonymous credentials in authentication, rendering it even more complex to handle misbehavior in VANETs, since the user identity is hidden and cannot be linked arbitrarily which curbs the punishment of misbehaving users.

Our contributions. Given the conflicting goals of privacy and traceability, and the challenges in designing a privacy-preserving defense scheme for VANETs, we are motivated to propose a security system that can effectively and efficiently solve the conflicts and challenges. Specifically, our main contributions in this paper include:

1. We propose a pseudonym-based scheme to assure vehicle user privacy and traceability.

- *J. Sun is with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996. E-mail: jysun@eecs.utk.edu*
- *C. Zhang and Y. Fang are with the Department of Electrical and Computer Engineering, University of Florida, 435 New Engineering Building, PO Box 116130, Gainesville, FL 32611. E-mail: zhangchi@ufl.edu, fang@ece.ufl.edu.*
- *Y. Zhang is with the Department of Electrical and Computer Engineering, 213 Electrical & Computer Engineering Center (ECEC), New Jersey Institute of Technology University Heights, Newark, NJ 07102. E-mail: yczhang@njit.edu.*

Manuscript received 19 Aug. 2009; revised 24 Nov. 2009; accepted 25 Nov. 2009; published online 8 Jan. 2010.
Recommended for acceptance by Y.C. Tseng.
For information on obtaining reprints of this article, please send e-mail to: tpds@computer.org, and reference IEEECS Log Number TPDS-2009-08-0376.
Digital Object Identifier no. 10.1109/TPDS.2010.14.

2. We design a threshold signature-based scheme to achieve nonframeability in tracing law violators. In this scheme, an innocent vehicle cannot be framed by a corrupted law enforcement authority due to our role-splitting mechanism.
3. A novel privacy-preserving defense scheme is proposed leveraging threshold authentication. It guarantees that any additional authentication beyond the threshold will result in the revocation of the misbehaving users. Our defense scheme differs from others mainly in that it yields flexibility in the revocation (i.e., not all types of misbehavior should be punished). Moreover, the dynamic accumulators in the threshold authentication technique [10] facilitates each user to place further restrictions (besides the threshold) on other communicating users, which is an attractive feature to service providers.
4. Our design incorporates mechanisms that guarantee authentication, nonrepudiation, message integrity, and confidentiality.
5. We provide comprehensive analysis to show the fulfillment of the security objectives and the efficiency of the proposed system.

In what follows, we use law violators (or violators) and misbehaving users to describe VANET users who misbehave in the law enforcement scenario and the infrastructure access scenario, respectively.

Organization. The rest of this paper is organized as follows: A survey of related work is provided in Section 2. Section 3 introduces some preliminaries relevant to our work. Section 4 describes the system model including the entities and procedures involved in our schemes, and the security requirements. Section 5 elaborates on the schemes for achieving privacy and traceability, and nonframeability in tracing, as well as the privacy-preserving defense scheme. Security and efficiency analysis of the proposed system are the focus of Sections 6 and 7, respectively. Section 8 concludes the paper.

2 Related Work

There is a large body of research work related to the security and privacy in VANETs. The most related works are on the design of privacy-preserving schemes. Raya and Hubaux [3] investigated the privacy issue by proposing a pseudonym-based approach using anonymous public keys and the public key infrastructure (PKI), where the public key certificate is needed, giving rise to extra communication and storage overhead. The authors also proposed three credential revocation protocols tailored for VANETs, namely RTPD, RC^2RL, and DRP [11], considering that the certificate revocation list (CRL) needs to be distributed across the entire network in a timely manner. All the three protocols seem to work well under conventional public key infrastructure (PKI). However, the authors also proposed to use frequently updated anonymous public keys to fulfill users' requirement on identity and location privacy. If this privacy preserving technique is used in conjunction with RC^2RL and DRP, the CRL produced by the trusted authority will become huge in size, rendering the revocation protocols highly inefficient. A lightweight symmetric-key-based security scheme for balancing auditability and privacy in VANETs is proposed in [4]. It bears the drawback that peer vehicles authenticate each other via a base station, which is unsuitable for intervehicle communications. Gamage et al. [12] adopted an identity-based (ID-based) ring signature scheme to achieve signer ambiguity and hence fulfill the privacy requirement in VANET applications. The disadvantage of the ring signature scheme in the context of VANET applications, is the unconditional privacy, resulting in the traceability requirement unattainable. Group signature-based schemes are proposed in [8], [13], [14], where signer privacy is conditional on the group manager. As a result, all these schemes have the problem of identity escrow, as a group manager who possesses the group master key can arbitrarily reveal the identity of any group member. In addition, due to the limitation of group formation in VANETs (e.g., too few cars in the vicinity to establish the group), the group-based schemes [8], [13], [14], [15] may not be applied appropriately. The election of group leader will sometimes encounter difficulties since a trusted entity cannot be found amongst peer vehicles. Kamat et al. [16], [17] proposed an ID-based security framework for VANETs to provide authentication, nonrepudiation, and pseudonymity. However, their framework is limited by the strong dependence on the infrastructure for short-lived pseudonym generation, which renders the signaling overhead overwhelming. The proposed nonrepudiation scheme enables a single authority to retrieve the identity which may raise the concern on potential abuse. Schemes leveraging pseudonyms in VANETs can also be found in [7], [18] with the revocation feasible in limited settings, and in [19] where the certificate authority maintains mapping from an identity to the set of vehicle-generated pseudonyms.

There are also a number of defense techniques against misbehavior in VANET literature besides those in [3]. An indirect approach via the aid of infrastructure is used in [8] and [16]. The TA distributes the CRL to the infrastructure points which then take over the TA's responsibility to execute the revocation protocol. The advantage of this approach is that vehicles never need to download the entire CRL. Unfortunately, the conditional anonymity claimed in [8] and [16] only applies to amongst peer vehicles, under the assumption that the infrastructure points (group manager in [8] and base station in [16]) are trusted. The infrastructure points can reveal the identity of any vehicle at any time even if the vehicle is honest. The scheme in [9] leverages a single TA to recover the identity of a (possibly honest) vehicle, where revocation issues are not discussed. Recently, Tsang et al. [20] proposed a blacklistable anonymous credential system for blocking misbehavior without the trusted third party (TTP). The blacklisting technique can be applied to VANETs as: if the vehicle fails to prove that it is not on the blacklist of the current authenticator, the authenticator will ignore the messages or requests sent by this vehicle. Although not proposed specifically for VANETs, the proposal in [20] has a similar claim as ours that the capability of a TTP (network authority in our paper) to recover a user's identity in any case is too strong a punishment and highly undesirable in some scenarios. The downside of this technique is the lack of options to trace misbehaving users, since any user in the system (misbehaving or not) will by no means be identified by any entity including the authorities.

We proposed a privacy-preserving defense scheme against misbehavior in [21] leveraging threshold authentication technique. This scheme and the scheme in [7] both preserve user privacy, and simultaneously provide traceability (i.e., tracing law violators by enforcement authorities in [7] and tracing misbehaving users by network authorities in [21]). The major differences between these schemes are the different technical realizations of the privacy and traceability schemes, due to the different application scenarios and detailed security requirements. In this paper, we incorporate the schemes in [7] and [21] to propose a security system that aims at achieving user privacy and traceability, taking into account different types of authorities in VANETs, and their requirements for traceability. Furthermore, we extend the previous works by offering detailed efficiency analysis in terms of storage, computation, and communication in the proposed system.

3 Preliminaries

This section comprises basic introduction to the cryptographic system and primitives used as building blocks in our security system.

3.1 ID-Based Cryptography (IBC)

Identity-based or ID-based cryptosystem 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. Boneh and Franklin [22] 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 properties:

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

IBC schemes are used mainly for encryption, authentication, and nonrepudiation in our VANET system. Compared to the conventional PKI (public key infrastructure), IBC infrastructure avoids the use of certificates for public key verification and the exchange of public keys (and associated certificates), greatly improving the computation and communication efficiency.

3.2 Threshold Schemes Based on Secret Sharing

Threshold schemes are used as cryptographic means to distribute secret information to multiple entities to eliminate power centralization and a single point of failure. In [23], Shamir considered the problem of dividing some information I into n pieces $I_1, \ldots, I_n$, such that knowledge of any k or more of these $I_i (i \in [1, n])$ pieces can recover I while knowledge of $k - 1$ or fewer pieces keeps I completely undetermined [23]. Such a scheme is referred to as a (k, n) threshold scheme which is computed based on polynomial interpolation. Define a $k - 1$ degree polynomial $y(x) = a_0 + \sum_{i=1}^{k-1} a_i x^i$ with $a_0 = I \in G_1$, where $a_1, \ldots, a_{k-1}$ are randomly chosen from G_1. Let $I_i = y(i), i \in [1, n]$ and $\Phi \subseteq \{I_1, \ldots, I_n\}$ with $|\Phi| \geq k$, where $|\cdot|$ denotes the cardinality of the given set. The I_i values in Φ and the indices i can be used to reconstruct the original information $I = y(0) = a_0$ by computing $y(x) = \sum_{j\in\Psi} \rho_{xj}^{\Psi} I_j$, where $\rho_{xj}^{\Psi} = \prod_{l\in\Psi, l\neq j} \frac{x-l}{j-l} \in Z_q$ is the Lagrange coefficient for a set $\Psi \subseteq \{1, \ldots, n\}$ with $|\Psi| \geq k$. This technique is used in the design of the nonframeability scheme for law enforcement authorities.

3.3 Proof of Knowledge

A proof of knowledge is an interactive proof where the prover convinces the verifier of the validity of a statement. In the case of a zero knowledge proof of knowledge, the above interactive proof is carried out without the prover revealing any information used to prove the statement. Let G be a cyclic group with generator g where solving the discrete logarithm is intractable. G is of prime order p. One can prove the knowledge of the discrete logarithm $x \in Z_p$ with respect to y in base g as $PK\{(x) : y = g^x\}$, which is the so-called Σ-protocol of three move structure: commitment, challenge, and response. Schnorr [24] first provided a construction for the Σ-protocol. The threshold authentication technique used in this paper as the defense against misbehavior is based on the Σ-protocol for zero knowledge proof. The proof of knowledge techniques are mainly used for the threshold-authentication-based defense scheme.

4 System Model

We describe the functionalities of our security system and define security requirements in this section.

4.1 Overview

Major entities in a VANET environment are depicted in Fig. 1. As mentioned before, traceability is needed by law enforcement authorities (LEAs) who require the identity of a violating vehicle to be disclosed for investigating the cause of accidents or crimes. Due to the seriousness of liability issues, if a single authority (e.g., the police) is fully capable of revealing the vehicle identity, this privilege may be abused. It is desirable if two or more authorities (e.g., the police, judge, special agents, and other possible law enforcement authorities) are granted distributed control over the identity retrieval process. One benefit in doing so is that corrupted authorities (the number being less than the threshold) cannot arbitrarily trace vehicle users to compromise their privacy. Another benefit is that malicious authorities cannot falsely accuse (or frame) honest users. Such role-splitting is not required for network authorities since the threshold authentication technique in our defense scheme prevents a network authority from falsely accusing honest users. The proposed security system primarily consists of techniques addressing the privacy, traceability, nonframeability, and revocation (only by network authorities) issues.

The logic diagram of the entities' interactions is depicted in Fig. 2, where the arrowed lines indicate the direction of packet flow or physical communications, the bracketed numbers near each line index the major events or procedures between the connected entities. The vehicle users are further

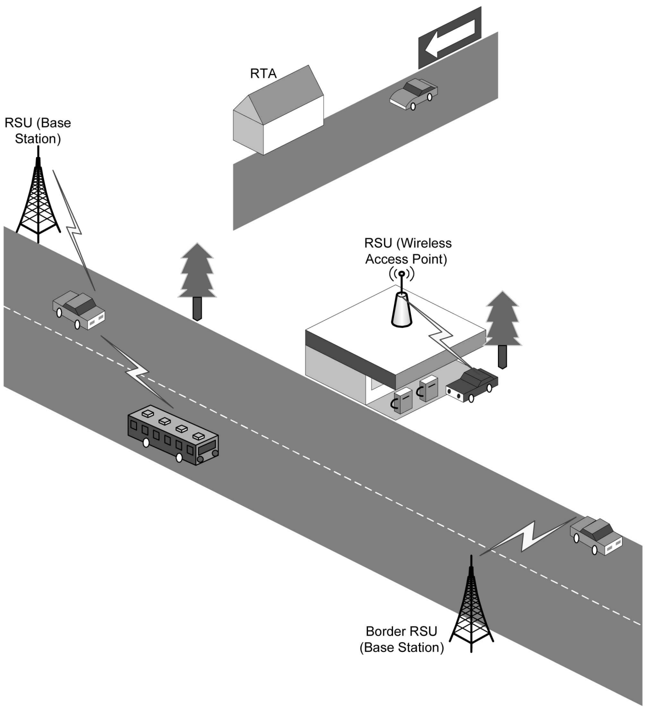


Fig. 1. A VANET system.

split into access group owners and members, whereas the RSUs can only be access group owners. The entities and events/procedures are described in what follows.

4.2 Entities and Procedures

The entities in our system are the regional transportation authorities (RTAs), law enforcement authorities (LEAs), network authorities, roadside infrastructure including border RSUs for pseudonym management and regular RSUs (simply RSUs) for Internet access, and vehicle users. Considering practical scenarios, the RSUs in our system are mainly responsible for providing infrastructure access and network services. The RSUs are assumed to be operated by third-party service providers (SPs) who have business contracts with the RTA to build access infrastructure in the RTA's region. The RSUs are thus not owned by the RTA and have no pre-established trust relationship with the RTA. On the other hand, borders RSUs are owned and operated by the RTA, and can be considered as the agents who are delegated with the RTA's authority. These entities are involved in the following procedures:

System setup: This procedure is executed by the RTA for initial VANET system setup including domain parameter publication, public/private key assignment for entities in the system to perform desired tasks, and database creation for storing necessary records (i.e., the pseudonym lookup table PLT).

Pseudonym generation and authentication for privacy: RTA and border RSUs execute this procedure to assign pseudonym/private key pairs to both vehicles traveling in their home domain and vehicles from other RTAs' domains, so that these vehicles are able to authenticate with RSUs and other vehicles to obtain services and useful messages.

Threshold signature for nonframeability: This procedure is invoked by LEAs to share the secret information for recovering a guilty vehicle's identity. Meanwhile, it prevents corrupted authorities from gathering full power to accuse an innocent vehicle. The functional component of this procedure is the threshold signature.

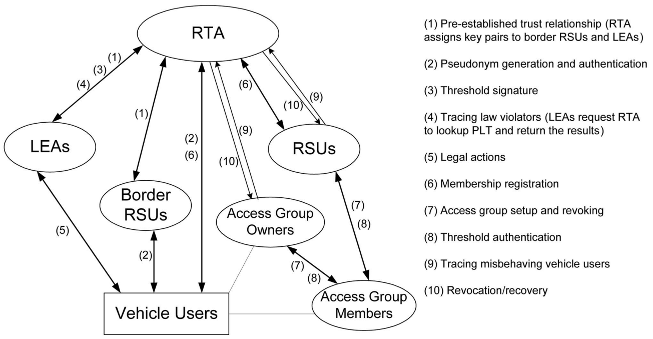

RTA
LEAs
Border RSUs
Access Group Owners
RSUs
Vehicle Users
Access Group Members
(1)
(3)
(4)
(1)
(2)
(6)
(9)
(10)
(6)
(10)
(9)
(5)
(2)
(7)
(8)
(7)
(8)
(1) Pre-established trust relationship (RTA assigns key pairs to border RSUs and LEAs)
(2) Pseudonym generation and authentication
(3) Threshold signature
(4) Tracing law violators (LEAs request RTA to lookup PLT and return the results)
(5) Legal actions
(6) Membership registration
(7) Access group setup and revoking
(8) Threshold authentication
(9) Tracing misbehaving vehicle users
(10) Revocation/recovery

Fig. 2. Logic diagram of interrelations and interactions.

Threshold-authentication-based defense: Designed for the network authorities, this procedure is used to revoke a misbehaving vehicle's credential, refraining the vehicle from further disrupting system operations. As the core of this procedure, the threshold authentication technique provides a mechanism to allow certain types of misbehavior that should not result in revocation. For instance, the misbehavior may be caused by malfunctioning hardware and thus is incidental. These types of misbehavior share a common feature, i.e., their occurrence or frequency is low, specifically, lower than a predetermined threshold. Threshold authentication-based defense further consists of six sub-procedures:

Membership registration: RSUs and vehicle users register with the RTA to use VANETs. Upon successful registration, a member public/private key pair (mpk, msk) is issued to each RSU and vehicles. The RTA associates the member's credential with the issued public key and includes this pair of information into a credential list ID_{list}.

Access group setup: RSUs and vehicles setup their own access groups, the member of which is granted privilege to communicate with the access group owner. The group owner adds members to the group and updates related public information. Each added member obtains an access key mak for the group.

Access group revoking: The access group owner revokes the granted privilege when deciding to stop communications with a member, due to some decision criteria for misbehavior. The access group owner removes the member from the access group and updates related public information.

Threshold authentication: This procedure is executed between an RSU and a vehicle, or between peer vehicles. We call the authenticator in this procedure Alice who announces the threshold k possibly different for each user being authenticated. The authentication succeeds if and only if the following conditions are met simultaneously: the user Bob authenticating with Alice is a registered member of the VANET system, Bob is a legitimate member of Alice's access group (if Alice is an access group owner) whose member privilege has not been revoked, and the authentication threshold has not been exceeded. Alice records the authentication transcripts in $AUTH_{log}$:

Tracing: This procedure is used by Alice to trace a misbehaving member M_n who attempts to authenticate more than k times. Alice relies on the $AUTH_{log}$ and public information, and obtains M_n's credential n as the procedure output which is reported to the RTA.

Revocation/recovery: Upon receiving the complaints from other entities in the system as the output of *Tracing*, the RTA decides if the misbehaving member's credential needs to be revoked. The RTA then performs the identity recovery by looking up the same pseudonym lookup table PLT (cf. ***System setup*** above) which also records the correspondence between the credential n and identity ID_n.

Note that for the ease of presentation, we assume the RTAs to act as network authorities for the defense scheme in this paper. In reality, when the roles of RTA and network authority are separate, the network authority can simply take charge as the RTA in the above subprocedures. Nonetheless, in the execution of *Revocation/recovery*, the network authority needs to establish trust with or be delegated by the RTA in order to access the PLT. When we mention network authorities in what follows, we implicitly refer to RTAs in the network authority role.

4.3 Security Requirements

We define the security requirements for our VANET security system, and will show the fulfillment of these requirements after presenting the design details.

1. Privacy: The privacy requirement states that private information such as vehicle owner's identity and location privacy is preserved against unlawful tracing and user profiling.
2. Traceability: It is required where the identity information of violators need be revealed by law enforcement authorities for liability purposes. The traceability requirement also indicates that a misbehaving user will be identified and the corresponding credential revoked, if necessary, by network authorities, to prevent this user from further disrupting system operations. Certain criteria have to be met for the traceability of a misbehaving user as explained in the next section.
3. Nonframeability: Nonframeability requires that no entity in the system can accuse an honest user for having violated the law or misbehaved.
4. Other requirements: A secure VANET system should satisfy several fundamental requirements, namely, authentication, nonrepudiation, message integrity, and confidentiality where sensitive information is being exchanged, to protect the system against unauthorized-message injection, denial of message disseminations, message alteration, and eavesdropping, respectively. Nonrepudiation also requires that violators or misbehaving users cannot deny the fact that they have violated the law or misbehaved.

5 The Proposed Security System

This section elaborates on the technical design of the proposed security system.

5.1 System Setup

In our system, a trust domain is managed by a regional transportation authority (RTA). Different among countries, the region can be a state, province, etc. On input of 1^ι, the unary representation of the security parameter ι, the key generator outputs a tuple (G_1,G_2,e,P,q) as defined in Section 3.1. The RTA randomly selects a domain master secret $s \in_R Z_q^*$ to generate private keys associated with the ID-based public keys for each entity (i.e., vehicles, RSUs, other authorities) involved in VANET communications within the trust domain. The RTA then publishes its certified domain parameters $(q, G_1, G_2, e, P, P_{pb}, H_1)$, where $P_{pb} = sP$ and H_1: $\{0,1\}^* \rightarrow G_1$ is a cryptographic hash function. For the defense scheme, the RTA chooses $P_0, P_1, P_2, H \in G_1$, $\alpha \in_R Z_q^*$, and computes $P_{pub} = \alpha P$, $A = e(P,P)$. The RTA sets the group public and private keys as $gpk = (P, P_{pub}, P_0, P_1, P_2, H, A)$ and $gsk = \alpha$, respectively. Furthermore, the RTA maintains and publishes ID_{list} which can be accessed by any user of the system.

A vehicle V's public/private key pair in this domain is assigned by the RTA as PK_v/Γ_v, with $PK_v = H_1(PS_v)$ and $\Gamma_v = s \cdot PK_v$. Each RSU for network access in the RTA's domain will be assigned a key pair in a similar fashion, except that the RSU just uses the real identity as the public key. For privacy preserving purpose, vehicles always use their pseudonyms for VANET communications instead of real identities. The pseudonym plays the same role as the real identity in authentication and secure communications, which in our system is of the form:

$$PS_v := (Pseudonym, ExpiryDate)@RG_H, \qquad (1)$$

where $ExpiryDate$ defines the valid period of this PS_v, and RG_H denotes the home region where the vehicle is registered. As a result, the vehicles with public/private key pairs assigned by a same RTA (i.e., using the same master secret s) are capable of mutual authentication. Furthermore, the RTA will maintain a PLT (pseudonym lookup table) for each registered vehicle in its domain which consists of the correspondence of the real identity and the assigned pseudonyms, and can be accessed by the RTA's border RSUs.

The home region is assumed to be the most likely activity region of a vehicle. As the vehicle travels across regions, it needs public/private key pairs assigned by foreign regions (RG_F) typically with different master secrets, to remain authenticated in these regions in order to continue enjoying VANET services. This can be done by border RSUs owned by RTAs. In particular, each border RSU is operated by one RTA and will have multiple public/private key pairs, each issued by an adjacent RTA. The border RSU will be able to authenticate visiting vehicles based on the region information (i.e., RG_H, RG_F) carried in their pseudonyms, if the border RSU possesses a proper key pair. Upon successful authentication with the vehicle, the border RSU will issue pseudonym key pairs that can be used in the foreign region. There are several ways for the border RSU to issue valid key pairs. First, it can be configured with its RTA's master secret s which will be used to generate private keys corresponding to arbitrarily chosen public keys. This approach offers flexibility at the cost of higher risks in terms of compromising the domain master secret. Alternatives would be that the RTA configures the border RSU with pregenerated key pairs for future assignment without releasing s, or the adoption of the pseudonym self-generation technique proposed in [25] at the border RSU so that the above configuration can be skipped. A common drawback of these alternatives is the limitation of the pseudonym selection, i.e., the regional information that is imperative in our proposed security system cannot be arbitrarily incorporated into the pseudonym. We argue that since using tamper proof device at the border RSU will reduce the risk of the master secret disclosure, we will employ the first approach in our system. Specifically, a border RSU assigns key pairs in one of the following two ways:

1. The vehicle submits its pseudonym PS_v currently in use to the border RSU, which updates PPLT, a foreign lookup table maintained by the foreign RTA, to record the correspondence between PS_v and the newly assigned pseudonyms. Or,
2. after authenticating with the border RSU using the above PS_v, the vehicle submits its real identity ID_v (bearing the same form as (1)) in ciphertext to the border RSU, which updates the home RTA-maintained PLT to record the correspondence between ID_v and the newly assigned pseudonyms.

Let the pseudonym assigned for RG_F by the border RSU be of the form:

$$PS_v^f := (Pseudonym, ExpiryDate)@RG_H@RG_F. \quad (2)$$

The generation of the pseudonym key pair is analogous to that for RG_H. When the vehicle enters a region where the border RSU has no proper key pairs to authenticate this vehicle, the border RSU will contact the home RTA for further actions (e.g., requesting a valid key pair from the home RTA to authenticate with the vehicle). We will omit further discussion on this issue since it is not a key design issue in our system. We assume pre-established trust relationship and secure channel between RTAs, which can be achieved by any public key cryptosystems. We will primarily focus on the authentication and possible secure communications during intervehicle message exchange and infrastructure access.

5.2 Pseudonym-Based Techniques for Privacy

Since ring signature and group signature techniques for ensuring user privacy are unsuitable for our VANET system as mentioned in Section 2, we adopt the privacy preserving technique based on pseudonyms. In this paper, we do not assume the existence of pervasive VANET infrastructure and will rely on available wireless networks whenever possible.

5.2.1 Pseudonym Generation

Unlike sensors and some mobile nodes, storage is not a stringent requirement for vehicles, rendering the preloading of a large pool of pseudonyms feasible. Raya and Hubaux [3] quantitatively studied the storage space requirement for preloading anonymous keys (i.e., pseudonyms) and associated certificates for long term use (i.e., one year). Their results are obtained based on quantifying the upper and lower bounds on the pseudonym change interval for maintaining a satisfactory degree of privacy. We adopt the preloading method in our ID-based VANET system where a pool of shorter-lived pseudonyms is loaded into the vehicle by the RTA at the time of registration. The pool will be replenished in a shorter period which may be a month, week, or even a day. The merit of our approach is that considering the unavailability of the dedicated infrastructure for VANETs, the preload-and-replenish mechanism can be realized through the existing wireless infrastructure, such as Wi-Fi networks, wireless mesh networks (WMNs), etc. For instance, when the network is accessible and less busy some time close to an update, the pseudonym pool will be replenish via the secure channel between the vehicle and RTA or border RSUs after proper authentication. If the vehicle is requesting pseudonym update in the home region, the real identity ID_v will be indicated in ciphertext to the home RTA, which will then update the PLT. When the vehicle is requesting the pseudonym update in a foreign region, the obsolete pseudonym at the time of entering PS_{v_ob} (used for recording the correspondence with the newly assigned pseudonyms) will be indicated in ciphertext to the foreign RTA, which will update the PPLT accordingly. The pseudonym revocation list which will be much smaller in size than the credential revocation list (CRL) in [3], can also be downloaded using the available wireless infrastructure when the dedicated infrastructure is not yet pervasive. In addition to the preload-and-replenish mechanism, we base our system on the ID-based cryptosystem so that the vehicle need only store the pseudonym (public key), which saves the storage space required for certificates as in the conventional PKI-based systems [3].

5.2.2 Pseudonym Authentication

Equipped with sufficient pseudonyms, a vehicle can update its credential frequently enough to preserve privacy (cf. [3]). An important feature of VANET security is the digital signature as a building block. Whether in intervehicle communications or infrastructure access, authentication is the basic requirement since only messages from legitimate users should be considered. Message confidentiality remains an option in VANETs depending on the specific application scenario. For instance, safety-related messages do not contain sensitive information and thus encryption is not needed [3]. In some other applications such as toll paying where vehicles obtain Internet services from RSUs, message confidentiality via encryption schemes may be desired. When a vehicle V attempts to broadcast a message m to peers or to request network access from RSUs, it simply sends out:

$$V \rightarrow *: PS_v, m, \mathcal{SIG}_{\Gamma_v}(m \parallel t),$$

where $*$ denotes all peer vehicles in the communication range or any RSU, $\mathcal{SIG}_{\Gamma_v}$ denotes the ID-based signature using V's private key Γ_v, and t is the current system time to prevent message replay attack [26]. Upon receiving the message, a peer vehicle or RSU is able to authenticate the sender by verifying the signature which also ensures message integrity.

Afterwards, a shared key can be derived locally at V and another vehicle or RSU, U, if further communications are desired (e.g., the two vehicles remain in each other's transmission range for a while).

$$\begin{aligned} K_{v-u} &= e(PK_u, \Gamma_v) \\ &= e(PK_u, PK_v)^s \\ &= e(\Gamma_u, PK_v) = K_{u-v}. \end{aligned} \tag{3}$$

This shared key will then be used in further authentication or secure communications where encryption is needed as follows:

$$V \rightarrow U\text{: } PS_v, \mathcal{SKE}_{K_{v-u}}(m), \mathcal{HMAC}_{K_{v-u}}(\mathcal{SKE} \parallel t),$$

where $\mathcal{SKE}_{K_{v-u}}$ denotes the symmetric key encryption using the shared secret key K_{v-u}, and $\mathcal{HMAC}_{K_{v-u}}$ denotes the keyed-hash message authentication code leveraging the same shared key.

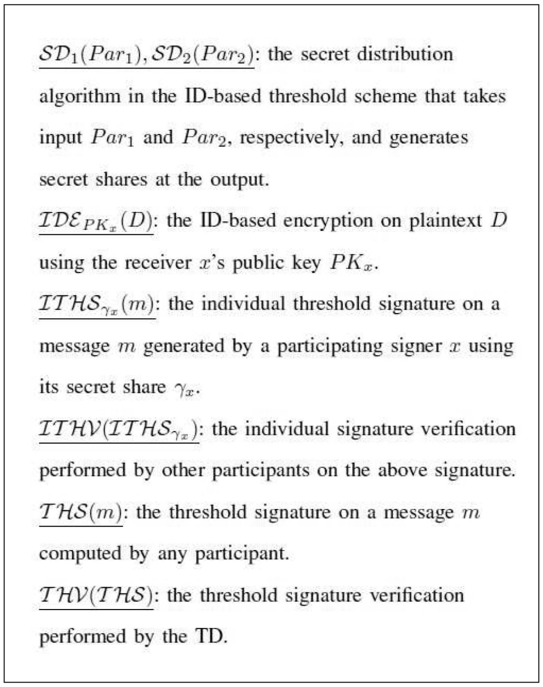
In the conventional PKI, the communicating vehicles need first exchange their public keys and certificates for authentication, during which the verifier has to verify the sender's signature on the message, as well as the certificate authority's signature on the sender's public key. After authentication, a shared key will be established mutually if desired for secure communications, where additional communication overhead is induced. In our ID-based system presented above, the sender merely sends one message (i.e., PS_v, m, $\mathcal{SIG}$), and the subsequent verification and symmetric key establishment can be performed without further interactions. Therefore, our system bears desirable features for satisfying security and efficiency requirements in VANETs.

5.3 Threshold Signature Techniques for Nonframeability

Applying the threshold-based secret sharing schemes to our system, the number of authorities for sharing the secret and for revealing the identity can be adjusted by setting different n and k values, respectively (cf. Section 3.2). These schemes offer great flexibility in several ways as stated in [23]. In this paper, we adopt ID-based threshold signatures to distribute the secret shares among designated authorities. The shares can be distributed by a trusted dealer (TD) which is the owner of the original secret. The TD takes one of its publicly known identifications (or the derived public key) Q_{TD} to be the user ID required as the input of the ID-based threshold signature scheme, and obtains the associated private key $\Gamma_{TD} = sQ_{TD}$ from the private key generator (PKG) as the original secret for sharing. We let $\gamma = \Gamma_{TD}$ for the description of the following threshold signature scheme. In our systme, the TD can be the RTA (i.e., PKG) or any other trusted entity who can run the secret distribution algorithm [27].

5.3.1 Corruption-Resistant Threshold Signing

Threshold signature schemes can be used in the scenario where the TD owns the secret and computes the shares (γ_i) to distribute among n designated authorities (e.g., the judge, police, other law enforcement authorities, etc.). When accidents or crimes occur, relevant messages exchanged can be extracted by the cooperating k or more authorities from the black-box-like device in vehicles which records pseudonyms used for the message exchanges. The participating authorities will jointly generate a secret κ without the TD, and will individually sign the pseudonym using their associated shares γ_i and κ_i. The resulting signatures from all other participants will be verified by individual participants. When at least k valid signatures are gathered, any participating authority can construct the threshold signature based on the k partial threshold signatures and submit it to the TD. The TD verifies the threshold signature on the pseudonym and will return the real identity corresponding to the pseudonym requested if the verification succeeds.



$\mathcal{SD}_1(Par_1), \mathcal{SD}_2(Par_2)$: the secret distribution algorithm in the ID-based threshold scheme that takes input Par_1 and Par_2, respectively, and generates secret shares at the output.

$\mathcal{IDE}_{PK_x}(D)$: the ID-based encryption on plaintext D using the receiver x's public key PK_x.

$\mathcal{ITHS}_{\gamma_x}(m)$: the individual threshold signature on a message m generated by a participating signer x using its secret share γ_x.

$\mathcal{ITHV}(\mathcal{ITHS}_{\gamma_x})$: the individual signature verification performed by other participants on the above signature.

$\mathcal{THS}(m)$: the threshold signature on a message m computed by any participant.

$\mathcal{THV}(\mathcal{THS})$: the threshold signature verification performed by the TD.

Fig. 3. List of notations in threshold signing procedure.

The procedure described above is demonstrated as follows where relevant notations are listed in Fig. 3, using the ID-based threshold signature in [27]:

1. TD uses $\mathcal{SD}_1(\gamma, k, n, Other)$ to generate secret shares γ_i, $\forall i \in [1, n]$, where $Other$ denotes some published parameters in the TD's domain.
2. TD sends PK_i, $\mathcal{IDE}_{PK_i}(\gamma_i)$, $\mathcal{SIG}_{\Gamma_{TD}}(PK_i \parallel \mathcal{IDE}_{PK_i} \parallel t)$ to AU_i, $\forall i \in [1, n]$, where PK_i is AU_i's public key.
3. All participants AU_i, $\forall i \in [1, n]$, run $\mathcal{SD}_2(k, n, G_1, P)$ to jointly generate κ.
4. Each participating AU_i generates partial threshold signatures $\mathcal{ITHS}_{\gamma_i}(PS)$ using γ_i and κ_i, where $i \in [1, n]$, and PS is the pseudonym requested for lookup.
5. Each participating AU_i broadcasts PS, $\mathcal{ITHS}_{\gamma_i}$, $\mathcal{SIG}_{\Gamma_{AU_i}}(PS \parallel \mathcal{ITHS}_{\gamma_i} \parallel t)$.
6. Each participating AU_i verifies the received signatures from all other participants AU_j using $\mathcal{ITHV}(\mathcal{ITHS}_{\gamma_j})$, $j \in [1, n], j \neq i$.
7. Any participating AU_i calculates $\mathcal{THS}(PS)$ based on $\mathcal{ITHS}_{\gamma_i}$, $\forall i \in \Omega$, where $\Omega \subseteq \{1, 2, \ldots, n\}$ with $|\Omega| \geq k$.
8. The above AU_i sends PS, $\mathcal{THS}$, $\mathcal{HMAC}_{\gamma_i}(PS \parallel \mathcal{THS} \parallel t)$ to TD.
9. TD verifies the threshold signature using $\mathcal{THV}(\mathcal{THS})$ and if successful, returns the real identity from the

pseudonym lookup table to participating AU_i with $PK_i, \mathcal{SKE}_{\gamma_i}(PS \parallel ID_v), \mathcal{HMAC}_{\gamma_i}(PK_i \parallel \mathcal{SKE}_{\gamma_i} \parallel t)$.

ID-based threshold signature schemes proposed in the literature [27], [28], [29] can be applied in our system to perform $\mathcal{SD}, \mathcal{ITHS}_{\gamma_i}, \mathcal{ITHV}, \mathcal{THS}$, and $\mathcal{THV}$ indicated in the above procedure.

5.3.2 Tracing Law Violators

Threshold signing is a prerequisite for tracing law violators, which involves authority collaboration and the RTA's assistance in pseudonym lookup in Step 9 above, if the TD is not the home RTA (e.g., the accident occurred and thus is investigated at a foreign region), the pseudonym lookup procedure may involve a single-step or a multistep lookup. If a PLT is looked up, the TD will retrieve the real identity of the vehicle based on the submitted pseudonym. On the other hand, if a PPLT is looked up, the TD will only retrieve the vehicle's obsolete pseudonym PS_{v_ob} at the time of entering and will transfer PS_{v_ob}, $\mathcal{THS}$, Q_{TD} to the vehicle's previously visited RTA according to the region information contained in PS_{v_ob}. Note that if the previous RTA is not the home RTA (i.e., the vehicle has entered from another foreign region), the previous RTA will follow a similar lookup procedure until the information $PS_{v_h}, \mathcal{THS}, Q_{TD}$ reaches the home RTA, where PS_{v_h} denotes the obsolete pseudonym originally assigned by the home RTA. The additional information $\mathcal{THS}$, Q_{TD} is included for the home RTA to verify the threshold signature. As a simple illustration, if the police and the judge are the designated authorities whose signatures are required to access the PLT (or PPLT), a $(2, 2)$ threshold signature scheme will suit.

5.4 Threshold Authentication-Based Defense Scheme

When misbehavior occurs during network access, network authorities require the revocation of misbehaving users and should not be able to arbitrarily trace honest users. It can be achieved only by defense schemes that offer privacy-preserving and traceability features. Furthermore, the key reason for adopting the threshold authentication technique is the capability to tolerate certain misbehavior due to the flexible *threshold*, in addition to the privacy and traceability guarantees. This functionality cannot be provided by the pseudonym-based approach. Consider malfunctioning vehicles as an example of nonmalicious misbehavior that should be tolerated to certain extent. Malfunctioning and intentional (or malicious) misbehavior are difficult to distinguish, which would require additional software installed in vehicles and RSUs to analyze the behavior of the message sender and to reach a decision. As a result, it is not an easy task to apply defense schemes differently for malfunctioning and "real" misbehavior. This is the reason that threshold authentication is employed in our defense scheme, where misbehavior can be tolerated as long as the number of times it occurs is less than the specified threshold. It is similar in purpose to the glitch protection proposed in [30]. In our example, within the threshold, if the malfunctioning vehicle finds out and recovers from the problem (e.g., via the automatic error warnings generated by the vehicle's on-board unit), this incidental misbehavior can be ignored (i.e., undetected) by the access group owner. Only when the vehicle cannot detect the malfunctioning, i.e., the vehicle constantly misbehaves, will the tracing and revocation be initiated by the access group owner. The malfunctioning vehicle's identity will be revealed with the aid from the RTA, and the vehicle will be informed about the malfunctioning system by the access group owner.

The technical details of the defense scheme will be presented below, followed by discussions on fine-grained defense leveraging access groups.

5.4.1 Membership Registration

After the initial system setup, each legitimate user is required to register (i.e., membership registration) with the RTA and become a member of the defense system, which is required for the threshold-authentication-based defense scheme. The registration is carried out by the user M_n randomly selecting $x', r \in_R Z_q^*$ and engaging in the following interactions with the RTA:

1. $M_n \rightarrow RTA$: $PS_{M_n}, C' = x'P + rH, t_1, \mathcal{HMAC}_{\pi}(C' \parallel t_1)$;
2. $RTA \rightarrow M_n$: $y, y' \in_R Z_q^*$, t_2, $\mathcal{HMAC}_{\pi}(y \parallel y' \parallel t_2)$;
3. $M_n \rightarrow RTA$: $(C, \beta) = (xP, A^x)$, ZKP_1, t_3, $\mathcal{HMAC}_{\pi}$ $(C \parallel \beta \parallel ZKP_1 \parallel t_3)$;
4. $RTA \rightarrow M_n$: $a \in_R Z_q^*$, $S = \frac{1}{\alpha + a}(C + P_0)$, t_4, $\mathcal{HMAC}_{\pi}$ $(a \parallel S \parallel t_4)$,

where C' is a commitment that will later be used in ZKP_1. At the end of this procedure, M_n checks if $e(S, aP + P_{pub}) = e(C + P_0, P)$ holds to ensure that his member public and private keys, $mpk = (a, S, C, \beta)$ and $msk = x$, respectively, are correctly formed. In Step 2, the RTA first authenticates M_n using M_n's pseudonym PS_{M_n} to ensure the legitimacy of M_n in the VANET system. In Step 3, M_n computes $x = y + x'y'$ and adds (n, β) to ID_{list}. Before Step 4, the RTA verifies the presence of (n, β) in ID_{list}, the validity of $\beta = e(C, P)$ and proof of knowledge ZKP_1 (refer to [10] for proof details). If the verification succeeds, the RTA will issue the member public key to M_n as shown in Step 4. The RTA will also link M_n's member credential n to his real identity ID_n by adding a column of n to the PLT, an exemplary entry in which will be (PS_{M_n}, ID_n, n). This linkage will be used for *Revocation/recovery* described later in this section.

5.4.2 Access Group Setup

A user opting for his own access group to place further restriction on other users acts as an access group owner. The access group owner selects $Q \in G_1, Q_1, Q_2 \in G_2, s \in_R Z_q^*$ and sets his public/private key pair as $(apk = (Q, Q_{pub}, Q_1, Q_2)$, $ask = s)$, where $Q_{pub} = sQ$. The access group owner maintains the following information: the $AUTH_{log}$, the accumulated value D [31] for automatically revoking access rights of the group members, and a public archive ARC of the form (a, b, D), where $b = 1, 0$ indicates the grant, revocation of an access group member, respectively. Initially, D is set to $D_0 \in G_1$, $AUTH_{log}$ and ARC are empty. A user M_n joins the access group owner's group as follows to further communicate with the access group owner (AGO):

1. $M_n \rightarrow AGO$: PS'_{M_n}, $mpk = (a, S, C, \beta)$, t_5, $\mathcal{SIG}_{\varpi'_{M_n}}$ $(mpk \parallel t_5)$;
2. $AGO \rightarrow M_n$: $PS_{AGO}, k, j, D_j, t_6, \mathcal{SIG}_{\varpi_{AGO}}(k \parallel j \parallel D_j \parallel t_6)$.

Note that we have used PS'_{M_n} here (serving the same purpose as PS_{M_n} in *Membership registration*) to indicate a possibly different pseudonym M_n is currently using. Suppose there are j tuples in ARC and accumulated value is D_j. After M_n joins the access group successfully, the access group owner updates the accumulated value to $D_{j+1} = (s+a)D_j$ and adds $(a, 1, D_{j+1})$ to ARC. M_n updates his/her access key to $mak = (j+1, W)$, where $W = D_j$, and initiates a running counter d which is compared with the threshold k to ensure that k is not exceeded each time the threshold authentication procedure is executed.

5.4.3 Access Group Revoking

The access group owner revokes M_n's access right when detecting misbehavior, which can be performed either at the time of M_n's joining (so M_n will not be granted access at all), or after the joining via the threshold authentication. The access group owner simply updates the accumulated value to $D_{j+1} = \frac{1}{s+a} D_j$ and adds $(a, 0, D_{j+1})$ to ARC. Group members must update the access key W based on a and the up-to-date accumulated value D_{j+1}, which ensures that a revoked member will be unable to obtain a valid W that passes the following threshold authentication.

5.4.4 Threshold Authentication

If M_n is an access group member of an access group owner (AGO), the threshold authentication takes place as follows:

$$M_n \rightarrow AGO : PS''_{M_n}, d, TAG, l \in_R Z_q^*, ZKP_2, t_7,$$
$$\mathcal{SIG}_{\varpi''_{M_n}}(d \parallel TAG \parallel l \parallel ZKP_2 \parallel t_7).$$

M_n computes TAG as $TAG = (\Gamma_d, \check{\Gamma}_d) = (\Theta_d^x, (A^l \check{\Theta}_d)^x)$, where $(\Theta_d, \check{\Theta}_d)$ is the dth tag base. In general, M_n computes the jth tag base by using a random oracle as $(\Theta_j, \check{\Theta}_j) = \mathcal{H}_{G_2 \times G_2}(PS_{AGO}, k, j)$ for $j = 1, \ldots, k$. The access group owner aborts the procedure if $d > k$, which ensures that the user cannot authenticate more than k times unless he/she reuses one or more of the k tag bases. Otherwise, the access group owner checks if TAG is different from all other entries in $AUTH_{log}$. If different and ZKP_2 is valid, the access group owner adds (TAG, l) and the proof of knowledge ZKP_2 (refer to [10] for proof details) to $AUTH_{log}$. In ZKP_2, the member proves possession or correct formation of (x, a, S, d, W) without revealing these parameters. If TAG already exists and ZKP_2 is valid, the access group owner proceeds to the tracing procedure below to detect the misbehaving user. If ZKP_2 is invalid, M_n is ignored and the procedure is aborted.

5.4.5 Tracing

In case there exist two entries (TAG, l, ZKP_2) and (TAG', l', ZKP_2') in the $AUTH_{log}$ that $\Gamma = \Gamma'$ and $l \neq l'$, the access group owner can trace a misbehaving user by computing $\beta = (\frac{\check{\Gamma}}{\check{\Gamma}'})^{\frac{1}{l-l'}} = A^x$. The ID_{list} maintained by the RTA can then be looked up to find the entry (n, β). M_n's credential n will eventually be recovered and reported to the RTA. The access group owner can also broadcast a warning message containing M_n's mpk (i.e., β) and the two entries shown above (for verification purpose) in his vicinity to inform the neighbors who will most likely be affected by the misbehavior. The neighbors may choose to ignore this warning message, or revoke M_n's access right to their access groups (if any). Note that the access group owner and his neighbors who noticed the misbehavior of M_n can lower the threshold on future authentications with M_n, when this M_n attempts to perform authentication using his member public key mpk, alleviating the effect of potential attacks launched by M_n during the vulnerable period.

5.4.6 Revocation/Recovery

Since n does not reveal any information on M_n's real identity, other users in the VANET system (except the RTA) cannot identify M_n as a misbehaving user. It is left to the RTA to decide wether to revoke M_n based on multiple criteria. One criterion may be to accumulate a certain number of reports against a same user. When the decision is reached to revoke a misbehaving user, the RTA checks the PLT for the entry (ID_n, n) and the user with identity ID_n will be restrained from future communications in the VANET system. Note that we have assumed the RTA is trustworthy and will only execute this procedure when a user truly misbehaves. However, this assumption may be too strong in realistic applications where the RTA can be corrupted. We can use a similar method as in [7] to split the role of the RTA (e.g., to include vehicle manufacturer) by leveraging the secret sharing technique to avoid the consequence of power centralization and a single point of failure.

5.4.7 Discussion

The access group setup and revoking procedures in the defense scheme enable the group owner to employ fine-grained defense against misbehaving group members, besides the threshold k not being exceeded. Specifically, the access group owner restricts his access group members in two cases: 1) the access group owner needs to control the activity duration of an access group member in addition to the number of times k, and 2) the access group owner decides to revoke an access group member's access right at any time during the threshold authentication after the threshold k has been announced to the member, possibly due to the severity of the member's misbehavior. An example of 1) can be when the access group owner is an RSU who provides services (e.g., infotainment) bearing an expiration time. In this case, the RSU may initiate a timer at the time a user joins the access group and deny the member's access by updating D_{j+1} based on a and the expired timer, even if k has not been reached. In the case of 2), the access group owner has more control over group members such as public vehicles that tend to impact greatly on victims [32]. The owner may revoke these members' access as soon as the severity of their misbehavior is raised above the tolerable level which is design specific and will not be elaborated here. However, Case 2) requires an extra proof of knowledge that the misbehavior is *not* up to the owner-specified severity level, which will not be further discussed in this paper due to space limitations.

6 Security Analysis

Our secure VANET system, which primarily strives to resolve the conflicts of privacy and traceability, also satisfies the requirements of authentication, message integrity, and confidentiality.

Privacy: Privacy is achieved by the pseudonym-based technique, as detailed in Section 5.2. The adoption of pseudonyms in VANET communications conceals the real identity of vehicles such that peer vehicles and RSUs cannot identify the sender of a specific message while are still able to authenticate the sender. By frequently updating the pseudonyms during communications, our system successfully defends legitimate vehicles against tracing and user profiling, assuming an underlying Tor-like anonymous network layer [33] which ensures location privacy.

To elaborate on the the achievable privacy, when a vehicle applies for pseudonyms using its real identity from either the RTA or border RSUs, its privacy cannot be guaranteed because the real identity must be revealed at these moments. However, after the pseudonym issuance, the vehicle will interact primarily with the service provider owned RSUs for Internet access, or with peer vehicles using the assigned pseudonyms. Since interactions using these pseudonyms with the RTA or border RSUs are minimal in our schemes, we can safely claim that the RTA cannot arbitrarily link pseudonyms with the identity to compromise the privacy of an honest vehicle user. The minimal interactions include: 1) the vehicle authenticates with the RTA in *Membership registration* which occurs only once if the vehicle is not traced or revoked, and 2) the vehicle authenticates with the border RSUs to obtain new pseudonym key pairs while in the specific region, which happens once every user-specified update period as mentioned in Section 5.2.1. By adjusting the length of the update period, the vehicle users can control the achievable privacy by limiting the border RSUs' chances to view the assigned pseudonyms. For example, a user can choose to preload and replenish pseudonym key pairs for a longer time (i.e., once every month), where the frequency of linking a pseudonym to an identity is lower and the achievable privacy level will be higher. On the other hand, if the user sacrifices privacy for storage efficiency, he/she can choose to update key pairs once every day. In this case, the border RSUs will be able to learn the identity of the user every day at the time of key updates. This is a common issue in the design of security schemes where tradeoff between security and efficiency will be involved. Note that due to the anonymous network layer, the border RSUs are unable to learn the location (i.e., network address) of this user.

Furthermore, in the defense scheme, a vehicle member's fixed member public key mpk is needed in the access group setup and revoking, and in the actual threshold authentication. Although mpk is not updated as pseudonyms, it will not be shown to the group owner in the authentication (cf. Section 5.4.4) where only the knowledge proof of the mpk is needed. Therefore, this fixed key will not enable the attackers to link multiple authentication events to a same vehicle user. Except for the cases where identities must be revealed to the authorities, no entity in our system can compromise the privacy of honest vehicle users.

Traceability: The pseudonym lookup tables PLT and PPLT enable the eventual tracing of law violators in the enforcement scenario, with the participation of law enforcement authorities and involvement of the RTA. The tracing procedure in the threshold authentication scheme guarantees the traceability of a misbehaving user who has authenticated more than k times during network access.

Nonframeability: The secret sharing technique in the threshold signature scheme ensures nonframeability in the case of corrupted authorities, who attempts to illegally recover an innocent user's identity. Moreover, it is not possible for any other entity in the system, especially the network authorities, to accuse an honest user for having misbehaved simply because an evidence (i.e., authentication transcripts) cannot be produced for verification by a third-party arbiter, in case disputes occur.

Authentication, Nonrepudiation, Integrity and Confidentiality: Authentication, nonrepudiation, and integrity are guaranteed by digital signatures (as shown in Section 5.2.2) which bound a message to a pseudonym and consequently the corresponding identity. If further interactions are needed and hence a symmetric key is established between interacting entities, integrity can be protected by utilizing the message authentication code (e.g., $\mathcal{HMAC}_{\gamma_i}$). Confidentiality is attained by using public or symmetric key encryptions, for the initial and subsequent secure communications, respectively.

Miscellaneous: Some other requirements pertinent to VANET security include data consistency, availability, position verification, efficiency, and scalability, and are discussed in [34], [35], [5], [36], [37] and [1], respectively. These requirements are not the security goals of our VANET system but can be fulfilled by applying the above techniques accordingly.

7 Efficiency Analysis

We carry out efficiency analysis in this section in terms of storage, computation, and communication efficiency for our security system.

7.1 Storage

In our system, the storage requirements on RTAs, other authorities, and RSUs are not stringent since these entities are distributed and resource-abundant in nature (e.g., there are many RTAs across the country, each of which may consist of several powerful servers). We are mainly concerned with the storage cost in vehicles due to the preloading of pseudonyms for privacy, and the information necessary for the defense scheme. Note that in *Threshold Signature Techniques for Nonframeability*, only law enforcement authorities are involved to split the authority role and no vehicle needs to participate in this procedure. Moreover, this procedure is invoked once for every accident or crime in which the guilty vehicle escapes from the scene. This event is expected to happen infrequently assuming a majority of vehicles are honest and responsible. Our system employs the combination of pseudonym preloading and replenishing, striving to reduce the storage cost at the vehicles compared to the preloading method alone. However, we assume the worst case (i.e., only preloading is available) for the following analysis. As shown in [3], the number of required pseudonyms per year is approximately 43,800, calculated based on the average driving time per day and the pseudonym update frequency for desired privacy. We adopt the parameters specified in [25] for our ID-based cryptosystem and a pseudonym/private key pair takes around 43 bytes using point compression ($2 \times |G_1|$

element) for storage. Each vehicle will be preloaded 1.88 M bytes per year, which is an acceptable size and outperforms the storage efficiency (3.5 M bytes per vehicle per year with 80 bytes per key/certificate) in [3]. The parameters (i.e., 100 bytes per key/certificate) chosen by [3] result in a security level similar to 2,048-bit RSA and a total storage space of 4.2 M bytes. In order to perform a fair comparison with our system, we derived the above 3.5 M bytes based on parameters yielding a security level equivalent to 1,024-bit RSA. Note that elliptic curve cryptography (ECC) based PKI was adopted by [3] and is well-known for its very efficient storage and communication performance due to small key sizes, compared to RSA-based PKI. If RSA-based PKI had been adopted, the total required storage space in the above scenario would be around 48.2 M bytes, assuming 1,024-bit RSA public key. Our ID-based cryptosystem shows advantage in terms of storage efficiency over ECC-based PKI in [3], let alone RSA-based PKI.

Furthermore, in our system, each vehicle needs to store a public/private key pair, roughly 214 bytes, for the defense scheme against misbehavior. When acting as an access group owner, the vehicle also stores $AUTH_{log}$ and public archive ARC containing records for each access group member. However, these two pieces of information will not grow in size over time due to the communication characteristics of VANETs, that is, vehicles have limited interaction time and interact only when staying in each other's vicinity. The likelihood of two vehicles encountering again in a short period (once they have been out of reach) is expected to be low. Additionally, the communicating vehicles during a reasonable time interval can be assumed of minimal change (e.g., a vehicle will most frequently exchange messages with neighboring vehicles in the same driving direction with similar driving speed). Therefore, the number of entries in $AUTH_{log}$ and ARC is maximally the largest possible number of vehicles in the transmission range in a given time interval. It is worth noting that the storage costs of PLT and PPLT at an RTA will not increase over time either, the reason being that each vehicle in the RTA's domain has exactly one entry in the PLT or PPLT. The RTA need not record all pseudonyms used by a vehicle but the effective one or those recently expired ones, based on the $ExpiryDate$ field in the pseudonym. These recorded pseudonyms serve mainly for recovering a guilty vehicle's real identity, and thus, previously expired pseudonyms are useless assuming the accident or crime will be investigated shortly after its occurrence.

7.2 Computation

Similar to the argument in the storage analysis, we are interested in the computation costs at vehicles which are least powerful in our system. Bilinear pairings are the most expensive operations when the ID-based cryptosystem is employed. Specifically, a vehicle needs to compute pairings for $\mathcal{SIG}_{\varpi_v}(m \parallel t)$ and K_{v-u} when exchange messages with other vehicles. The vehicle also needs to compute pairings for the defense scheme, where the zero knowledge proof (ZKP) construction and verification contribute to the highest cost since they must be performed each time an access group owner authenticates an access group member. Some pairing operations involved in *Registration* and *Access group setup* can be neglected due to the infrequent invocation of these procedures. For $\mathcal{SIG}_{\varpi_v}(m \parallel t)$, ID-based signature schemes such as [38] can be utilized for the signing and verification procedures. Using the techniques in [38], computation efficiency can be achieved by precomputing certain pairing operations and leaving a minimal number of pairings on-the-fly at the verification phase. One pairing operation is required for computing K_{v-u}, and only when the two vehicles remain in each other's transmission range. Regarding the ZKP-induced computation, the proofs can be constructed by access group members in advance and hence all pairings involved can be precomputed. In contrast, certain number of pairings must be computed in real-time while others can be precomputed for the verification performed by the access group owner. Employing the construction and verification shown in [10], four pairings need be computed by the access group owner in real time.

Although the computationally intensive pairing operations are not involved in conventional PKI (ECC-based PKI and RSA-based PKI), we argue that the ID-based cryptosystem based on pairings is still highly suitable, especially in our VANET environment. If Tate pairing is used for the basic pairing operation, it is shown in [39] that the time taken for computing a Tate pairing is 20 ms, 23 ms, and 26 ms, in the underlying base field of F_p (where $|p| = 512$ bit), $F_{2^{271}}$, and $F_{3^{97}}$, respectively. The first two fields have similar levels of security to 1,024-bit RSA while the last field has effective 922-bit security. Recent progress [40] shows that the computation time of Tate pairing on elliptic curves in characteristic 2 and 3 has been significantly improved, rendering pairing-based cryptosystems more realistic in security applications. Though vehicles are less powerful than other entities in our system (e.g., RTAs, RSUs, etc.), they have relatively high computation power (i.e., can be equipped with high-power processors) as a mobile device, in comparison with most other mobile devices such as cell phones, PDAs, or even laptops. Recent results show the feasibility of pairings on power-constrained smartcards [41], [42], which we believe strengthens our above argument. We conclude from the analysis that the real-time computation intensity in our system is highly acceptable even on the low-end mobile device.

7.3 Communication

Communication costs in our systems are mainly induced by broadcasts. Each message broadcast by vehicles (cf. Section 5.2.2) consists of a pseudonym (22 bytes), a plaintext message (disregarded in the comparisons), and a signature. The signature generated by the scheme in [38] is equivalent in size to an element in G_1 and an element in Z_q^*, which sum to roughly 43 bytes. As a result, each broadcasted message in our ID-based cryptosystem yields 65 bytes. If ECC-based PKI is adopted as in [3], each broadcasted message will consist of a signature and a certificate (one public key plus one signature), totaling 100 bytes. If the RSA-based PKI is adopted, each broadcasted message will induce up to 1.1 K bytes communication overhead (assuming the RSA key for signing is 1,024 bit or 128 byte, and a standard certificate comprising an RSA public key and the certificate authority's signature is roughly 1 K bytes). Apparently, our ID-based solution outperforms ECC-based PKI and has significant improvement compared to RSA-based PKI. The broadcast of partial threshold signatures by participating authorities for non-frameability takes place infrequently due to the rare case of escaping from the crime scene, as argued in the storage analysis. Another broadcast event in our system occurs at

Tracing in the defense scheme. Analogous to the broadcast of messages, this broadcast event, introducing roughly 1.2 K bytes, also takes place only in a vehicle's transmission range. As described in Section 5.4.5, this broadcast of the misbehaving vehicle's public key β and the two entries is optional, in that the access group owner can trace the misbehaving vehicle and report to the RTA without warning other vehicles in the vicinity. However, such warning is highly desirable in order to diminish the impact of misbehavior, sacrificing system performance for security. Improvement can be carried out by the access group owner only broadcasting the 128-byte β. Neighboring vehicles may choose to trust the access group owner from previous interactions and thus the two entries (of 1.1 K bytes) for verification purpose need not be broadcasted.

As a final remark, we point out that the characteristics of VANET systems determine that communication efficiency is the foremost performance indicator, among all the efficiency concerns. The reason is that vehicles, as the mobile devices in VANETs, are capable of intensive data storage and complex computation tasks, rendering the requirements for storage and computation efficiency less stringent. On the other hand, communication overhead will be overwhelming if inefficient design is carried out, due to potentially large user base (i.e., vehicles) in VANETs. Through the analysis of our system and those based on conventional PKI, we particularly demonstrate the promising performance regarding communication efficiency of our design built on ID-based cryptosystem. Moreover, limiting most communications to local interactions and not relying on pervasive infrastructure give rise to more affordable communication costs in our VANET system.

8 Conclusion and Future Work

We have presented the VANET security system mainly achieving privacy, traceability, nonframeability, and privacy-preserving defense against misbehavior. These functionalities are realized by the pseudonym-based technique, the threshold signature, and the threshold authentication based defense scheme. The ID-based cryptosystem facilitates us to design communication and storage efficient schemes. Through security and efficiency analysis, our system is shown to satisfy the predefined security objectives and desirable efficiencies. Our future work consists of simulating the proposed security system and experimenting it in real VANET settings.

Acknowledgments

This work was partially supported by the US National Science Foundation (NSF) under grants CNS-0916391, CNS-0716450, CNS-0721744, and CNS-0626881, and China 111 Project under grant B08038. The work of Yanchao Zhang was also partially supported by the NSF under grants CNS-0716302 and CNS-0844972 (CAREER).

References

[1] K. Plößl, T. Nowey, and C. Mletzko, "Towards a Security Architecture for Vehicular Ad Hoc Networks," *Proc. First Int'l Conf. Availability, Reliability and Security (ARES '06),* Apr. 2006.

[2] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks," *Proc. Fourth Workshop Hot Topics in Networks (HotNets IV),* Nov. 2005.

[3] M. Raya and J-P. Hubaux, "Securing Vehicular Ad Hoc Networks," *J. Computer Security,* special issue on security of ad hoc and sensor networks, vol. 15, no. 1, pp. 39-68, 2007.

[4] J.Y. Choi, M. Jakobsson, and S. Wetzel, "Balancing Auditability and Privacy in Vehicular Networks," *Proc. First ACM Int'l Workshop QoS and Security for Wireless and Mobile Networks (Q2SWinet '05),* pp. 79-87, Oct. 2005.

[5] T. Leinmüller, C. Maihöfer, E. Schoch, and F. Kargl, "Improved Security in Geographic Ad Hoc Routing through Autonomous Position Verification," *Proc. Third ACM Int'l Workshop Vehicular Ad Hoc Networks (VANET '06),* Sept. 2006.

[6] M.E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security Issues in a Future Vehicular Network," *Proc. European Wireless Conf. '02,* Feb. 2002.

[7] J. Sun, C. Zhang, and Y. Fang, "An Id-Based Framework Achieving Privacy and Non-Repudiation in Vehicular Ad Hoc Networks," *Proc. IEEE Military Comm. Conf.,* pp. 1-7, Oct. 2007.

[8] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications," *IEEE Trans. Vehicular Technology,* vol. 56, no. 6, pp. 3442-3456, Nov. 2007.

[9] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks," *Proc. IEEE INFOCOM,* pp. 816-824, Apr. 2008.

[10] L. Nguyen and R. Safavi-Naini, "Dynamic K-Times Anonymous Authentication," *Proc. Applied Cryptography and Network Security Conf.,* vol. 3531, pp. 318-333, 2005.

[11] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," *IEEE J. Selected Areas Comm.,* vol. 25, no. 8, pp. 1557-1568, Oct. 2007.

[12] C. Gamage, B. Gras, B. Crispo, and A.S. Tanenbaum, "An Identity-Based Ring Signature Scheme with Enhanced Privacy," *Proc. Second Int'l Conf. Security and Privacy in Comm. Networks (SecureComm '06),* Aug. 2006.

[13] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," *Proc. IEEE INFOCOM,* Apr. 2008.

[14] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs," *Proc. Sixth Ann. IEEE SECON Conf. (SECON '09),* 2009.

[15] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "Caravan: Providing Location Privacy for Vanet," *Proc. Embedded Security in Cars (ESCAR),* 2005.

[16] P. Kamat, A. Baliga, and W. Trappe, "An Identity-Based Security Framework for VANETs," *Proc. Third ACM Int'l Workshop Vehicular Ad Hoc Networks (VANET '06),* pp. 94-95, Sept. 2006.

[17] P. Kamat, A. Baliga, and W. Trappe, "Secure, Pseudonymous, and Auditable Communication in Vehicular Ad Hoc Networks," *J. Security and Comm. Networks,* vol. 1, no. 3, pp. 233-244, June 2008.

[18] J. Sun and Y. Fang, "Defense Against Misbehavior in Anonymous Vehicular Ad Hoc Networks," *Ad Hoc Networks,* vol. 7, no. 8, pp. 1515-1525, Nov. 2009.

[19] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and Robust Pseudonymous Authentication in VANET," *Proc. Fourth ACM Int'l Workshop Vehicular Ad Hoc Networks (VANET '07),* pp. 19-28, 2007.

[20] P. Tsang, M.H. Au, A. Kapadia, and S.W. Smith, "Blacklistable Anonymous Credentials: Blocking Misbehaving Users without TTPs," *Proc. ACM Conf. Computer and Comm. Security (CCS),* pp. 72-81, 2007.

[21] J. Sun and Y. Fang, "A Defense Technique Against Misbehavior in VANETs Based on Threshold Authentication," *Proc. IEEE Military Comm. Conf.,* Nov. 2008.

[22] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairings," *Advances in Cryptology-Asiacrypt,* Springer-Verlag, pp. 514-532, 2001.

[23] A. Shamir, "How to Share a Secret," *Comm. ACM,* vol. 22, pp. 612-613, 1979.

[24] C.-P. Schnorr, "Efficient Signature Generation by Smart Cards," vol. 4, no. 3, pp. 161-174, Jan. 1991.

[25] J. Sun, C. Zhang, and Y. Fang, "A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks," *Proc. IEEE INFOCOM,* pp. 1687-1695, Apr. 2008.

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

[27] J. Baek and Y. Zheng, "Identity-Based Threshold Signature Scheme from the Bilinear Pairings," *Proc. Int'l Conf. Information Technology (ITCC '04), Information Assurance and Security Track (IAS '04),* pp. 124-128, 2004.

[28] X. Chen, F. Zhang, D.M. Konidala, and K. Kim, "New ID-Based Threshold Signature Scheme from Bilinear Pairings," *Proc. Fifth Int'l Conf. Cryptology in India (INDOCRYPT '04),* 2004.

[29] J. Shao, Z. Cao, and L. Wang, *Efficient ID-Based Threshold Signature Schemes without Pairings,* Cryptology ePrint Archive, Report 2006/308, http://eprint.iacr.org/2006/308.pdf, 2006.

[30] J. Camenisch et al., "How to Win the Clonewars: Efficient Periodic n-Times Anonymous Authentication," *Proc. ACM Conf. Computer and Comm. Security (CCS),* pp. 201-210, 2006.

[31] J. Camenisch and A. Lysyanskaya, "Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials," *Proc. 22nd Ann. Int'l Cryptology Conf. (CRYPTO '02),* pp. 61-76, 2002.

[32] IEEE Std 1609.2-2006, *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments*ł Security Services for Applications and Management Messages, http://ieeexplore.ieee.org/servlet/opac?punumber=11000, 2006.

[33] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second-Generation Onion Router," *Proc. USENIX Security Symp.,* pp. 303-320, Aug. 2004.

[34] P. Golle, D. Greene, and J. Staddon, "Detecting and Correcting Malicious Data in VANETs," *Proc. First ACM Int'l Workshop Vehicular Ad Hoc Networks (VANET '04),* pp. 29-37, Oct. 2004.

[35] J. Yin, T. Elbatt, G. Yeung, B. Ryu, S. Habermas, H. Krishnan, and T. Talty, "Performance Evaluation of Safety Applications over DSRC Vehicular Ad Hoc Networks," *Proc. First ACM Int'l Workshop Vehicular Ad Hoc Networks (VANET '04),* Oct. 2004.

[36] T. Leinmüller, E. Schoch, and F. Kargl, "Position Verification Approaches for Vehicular Ad Hoc Networks," *Proc. IEEE Wireless Comm.,* pp. 16-21, Oct. 2006.

[37] M. Raya, A. Aziz, and J.P. Hubaux, "Efficient Secure Aggregation in VANETs," *Proc. Third ACM Int'l Workshop Vehicular Ad Hoc Networks (VANET '06),* pp. 67-75, Sept. 2006.

[38] F. Hess, "Efficient Identity-Based Signature Schemes Based on Pairings," *Selected Areas in Cryptography,* Springer-Verlag, pp. 310-324, 2002.

[39] P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott, "Efficient Algorithms for Pairing-Based Cryptosystems," *Proc. 22nd Ann. Int'l Cryptology Conf. (CRYPTO '02),* pp. 354-368, 2002.

[40] P.S.L.M. Barreto, S.D. Galbraith, C. ÓhÉigeartaigh, and M. Scott, *Efficient Pairing Computation on Supersingular Abelian Varieties,* Cryptology ePrint Archive, Report 2004/375, http://eprint.iacr.org/2004/375.pdf, Sept. 2005.

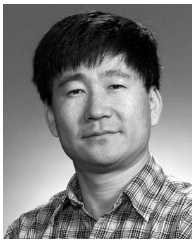
[41] M. Scott, N. Costigan, and W. Abdulwahab, *Implementing Cryptographic Pairings on Smartcards,* L. Goubin and M. Matsui, eds. Springer-Verlag, 2006.

[42] G.M. Bertoni, L. Chen, P. Fragneto, K.A. Harrison, and G. Pelosi, "Computing Tate Pairing on Smartcards," http://www.st.com/stonline/products/families/smartcard/ches2005_v4.pdf, 2005.

Jinyuan Sun received the BSc degree in computer information systems from Beijing Information Technology Institute, China, in 2003, the MASc degree in computer networks from Ryerson University, Canada, in 2005, and the PhD degree in electrical and computer engineering from the University of Florida, in 2010. She was a Network Test Developer at RuggedCom Inc., Ontario, Canada, 2005-2006. She has been an assistant professor in the Department of Electrical Engineering and Computer Science at University of Tennessee Knoxville since August 2010. Her research interests include the security protocol and architecture design of wireless networks.

Chi Zhang received the BE and ME degrees in electrical engineering from Huazhong University of Science and Technology, Wuhan, China, in July 1999 and January 2002, respectively. Since September 2004, he has been working toward the PhD degree in the Department of Electrical and Computer Engineering at the University of Florida, Gainesville. His research interests include network and distributed system security, wireless networking, and mobile computing.

Yanchao Zhang received the BE degree in computer communications from Nanjing University of Posts & Telecom, China, in 1999, the ME degree in computer applications from Beijing University of Posts & Telecom, China, in 2002, and the PhD degree in electrical and computer engineering from the University of Florida, Gainesville, in 2006. He has been an assistant professor in the Department of Electrical and Computer Engineering at New Jersey Institute of Technology since August 2006. His primary research interests include network and distributed system security, wireless networking, and mobile computing. He is an associate editor of the *IEEE Transactions on Vehicular Technology*, a feature editor of the *IEEE Wireless Communications*, and a guest editor of the *IEEE Wireless Communications* Special Issue on Security and Privacy in Emerging Wireless Networks. He is a TPC cochair of Communication and Information System Security Symposium, IEEE GLOBECOM '10. He is a winner of the US National Science Foundation (NSF) CAREER Award in 2009.



Yuguang Fang (S'92-M'97-SM'99-F'08) received the PhD degree in systems engineering from Case Western Reserve University in January 1994 and the PhD degree in electrical engineering from Boston University in May 1997. He was an assistant professor in the Department of Electrical and Computer Engineering at New Jersey Institute of Technology from July 1998 to May 2000. He then joined the Department of Electrical and Computer Engineering at the University of Florida in May 2000 as an assistant professor, got an early promotion to an associate professor with tenure in August 2003 and to a full professor in August 2005. He holds a University of Florida Research Foundation (UFRF) professorship from 2006 to 2009, a Changjiang scholar chair professorship with Xidian University, Xi'an, China, from 2008 to 2011, and a guest chair professorship with Tsinghua University, China, from 2009 to 2012. He has published more than 250 papers in refereed professional journals and conferences. He received the US National Science Foundation (NSF) Faculty Early Career Award in 2001 and the Office of Naval Research Young Investigator Award in 2002 and is the recipient of the Best Paper Award in IEEE International Conference on Network Protocols (ICNP) in 2006 and the recipient of the IEEE TCGN Best Paper Award in the IEEE High-Speed Networks Symposium, IEEE Globecom in 2002. He is also active in professional activities. He is a fellow of the IEEE and the IEEE Computer Society, and a member of the ACM. He is currently serving as an editor-in-chief for the *IEEE Wireless Communications* and serving/served on several editorial boards of technical journals including the *IEEE Transactions on Communications*, the *IEEE Transactions on Wireless Communications*, the *IEEE Wireless Communications Magazine*, and the *ACM Wireless Networks*. He was an editor for the *IEEE Transactions on Mobile Computing* and currently serves on its Steering Committee. He has been actively participating in professional conference organizations such as serving as the Steering Committee cochair for QShine from 2004 to 2008, the Technical Program vice-chair for IEEE INFOCOM '05, Technical Program Symposium cochair for IEEE Globecom '04, and a member of Technical Program Committee for IEEE INFOCOM (1998, 2000, 2003-2010), and ACM Mobihoc (2008-2009).