Ad Hoc Networks 7 (2009) 1515–1525

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Defense against misbehavior in anonymous vehicular ad hoc networks

Jinyuan Sun *, Yuguang Fang

Department of Electrical and Computer Engineering, University of Florida, P.O. Box 116130, Gainesville, FL 32611, United States

ARTICLE INFO

Article history:
Available online 3 May 2009

Keywords:
Misbehavior
Vehicular ad hoc networks (VANETs)
Anonymity
Privacy
Revocation

ABSTRACT

Vehicular ad hoc network (VANET) can offer various services and benefits to VANET users and thus deserves deployment effort. Misusing such network could cause destructive consequences. It is therefore necessary to discourage misbehavior and defend VANET systems against it, in order to ensure correct and smooth operations of the network. In this paper, we review the techniques for handling misbehavior in VANETs, particularly where anonymous communications are desired to conserve user privacy since it adds more complexity to the defense against misbehavior. A new scheme is proposed to punish misbehaving users and can be employed in both inter-vehicle and vehicle-to-infrastructure anonymous communications. Our scheme leverages some threshold authentication technique that dynamically revokes a user's credential, while providing the flexibility of whether to reveal the user's identity and tolerating unintentional misbehavior such as hardware malfunctioning.

Published by Elsevier B.V.

1. Introduction

Vehicular ad hoc networks (VANETs) are receiving research interests 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 [1–5]. Value-added services can enhance drivers' traveling experience by providing convenient Internet access, navigation, toll payment services, etc. [1,3–5]. More 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 [1–3,5,6]. 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 design and development of functional, reliable and efficient security architectures before all other implementation aspects of VANETs.

1.1. VANET security requirements

Fundamentally, VANET security design should guarantee authentication, data integrity, and in some specific application scenarios, confidentiality, to protect the network against unauthorized message injection, message alteration, and eavesdropping, respectively. An important feature of VANET security is the digital signature as a building block [3]. Whether in inter-vehicle communications or communications through infrastructure, authentication (using signatures) is a fundamental security requirement since only messages from legitimate senders will be considered. Signatures can also be used to guarantee data integrity (i.e., the message being sent is not modified). Another cryptographic method to achieve data integrity is through message authentication code (MAC), where a shared secret key is required at the two communicating entities. While fundamental to secure communications in many other networks, message confidentiality remains an option in VANETs depending on the specific

* Corresponding author. Tel.: +352 392 2746.
E-mail addresses: stellas@ufl.edu (J. Sun), fang@ece.ufl.edu (Y. Fang).

1570-8705/$ - see front matter Published by Elsevier B.V.
doi:10.1016/j.adhoc.2009.04.013

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 infotainment where vehicles obtain Internet services from the roadside infrastructure, message confidentiality via encryption schemes may be desired. Besides the fundamental security requirements, some other security aspects specific to VANETs also need consideration. These aspects include: (1) identity and location privacy preserving mechanisms against unlawful tracing and user profiling, (2) non-repudiation requirement when identity information need be revealed by law enforcing authorities for liability once accidents or crimes occur, (3) traceability by trusted network authorities (e.g., network administrator) for privilege revocation once misbehavior is detected, (4) non-frameability of an honest user who cannot be falsely accused of having misbehaved, (5) detecting and correcting malicious data to ensure data consistency, (6) position verification techniques to thwart position spoofing attacks, (7) suitable routing protocols for reliably delivering VANET traffic with real-time constraints, (8) efficiency and scalability of the security system, etc. Related surveys on different security aspects, requirements, and challenges of vehicular networks can be found in [3,2,7].

1.2. Misbehavior and defense in anonymous VANETs

Misbehavior takes place from time to time as a result of either intentional malicious behaviors (e.g., attacks) or hardware malfunctioning. It is less difficult to prevent misbehavior of unauthorized users of VANETs (i.e., outsiders) since legitimate users can simply ignore the messages injected by outsiders by means of authentication. Roadside infrastructure (i.e., base stations) can also use authentication to deny access and service requests from outsiders. This is one reason that we say digital signature is the building block of VANET security. On the contrary, misbehavior of legitimate users of VANETs (i.e., insiders) is more difficult and complex to prevent, the reason being that insiders possess the credentials issued by the authority to perform authentication with peer vehicles or base stations who can be easily tricked into trusting the insiders. Consequently, the insiders' misbehavior will have much larger impact on the network and be more devastating. Fortunately, certain techniques can be employed to detect such misbehavior and misbehaving users will be punished accordingly. Recently most proposals on VANET security [3,8,9] provide the option of using anonymous credentials in authentication while preserving traceability and revocation once such credentials are misused. Anonymous communications are desired due to users' increasing awareness and demand on their privacy protection. However, it is more complex to handle misbehavior in VANETs featuring anonymous communications between peer vehicles or between vehicles and infrastructure, since the user identity is hidden and cannot be linked arbitrarily which curbs the punishment of misbehaving users.

It is stressed that we are interested in the defense techniques against misbehavior which is assumed to be present. We do not attempt to discuss the techniques of detecting misbehavior since the detection of a problem (before it arises) is orthogonal to the solution of that problem (after it appears). We do not intend to define misbehavior either since it covers a broad spectrum of behavior that can be deemed as inappropriate or harmful and is application specific. For instance, misbehavior can be the dissemination of bogus messages, prevention of broadcast messages from reaching other vehicles, injection of irrelevant messages (e.g., spam), escaping from an accident (e.g., hit and run), improper use of network resource exceeding the allowed bandwidth, refusal of paying for services received from the network (e.g., pay per view in infotainment), or can be from a compromised vehicle controlled by an adversary, etc. Misbehavior also includes all other possible attacks launched to VANETs, the detail of which can be found in [3].

The rest of this paper is organized as follows. Section 2 surveys the existing techniques on the defense against misbehavior in VANETs. Section 3 describes the proposed defense scheme using threshold authentication technique. Analysis of the proposed scheme and comparisons among the defense techniques introduced in this paper are the topic of Section 4. Section 5 concludes the paper.

2. Defense techniques against misbehavior

Misbehavior considered here is with respect to legitimate users of VANETs whose behavior has greater impact on the system. Defense techniques against misbehavior in the existing literature fall into two categories.

CAT-I: In some scenarios, the misbehaving user's identity must be revealed. This is especially true in VANETs where liability is a concern. For instance, law enforcement departments require the vehicle identity to be disclosed for investigating the cause of accidents or crimes. The trusted authorities (TA) may require the same disclosure for punishing misbehaving vehicles of VANETs depending on the severity of the misbehavior and the policy for handling misbehavior implemented at the TA. An example of high severity misbehavior could be traffic jamming attack which can cause the entire network to collapse. It can be launched by some powerful and sophisticated attackers. The requirement of revealing identities implies that the privacy protection provided in VANETs should be *conditional* since otherwise a misbehaving user's identity can no longer be recovered.

CAT-II: On the other hand, certain types of misbehavior is not sufficiently severe for the misbehaving user's identity to be revealed, as in the case where the user misuses network resources (e.g., generating large amount of traffic beyond the bandwidth regulation while not causing jamming), or where the user disseminates spam or bogus messages that are not safety-related, etc. In these scenarios the network administrator (or service provider) and message receivers may simply block the misbehaving user from further communications and identity disclosure executed by the TA is not necessary. For one thing, this type of misbehavior can result from malfunctioning hardware and thus the user is not being malicious. In addition, different VANET users or administrators bear different expectations and definitions in terms of misbehavior. The allowance of

determining and blocking misbehaving users based on an individual's own discretion will yield flexibility and dynamics in VANET design.

Note that all the defense techniques mentioned in this paper are based on (different means of) credential revocation, which is the common way used to deprive misbehaving users' privilege and restrain these users from further misbehaving. The most popular technique to realize credential revocation is through the update and distribution of certificate revocation lists (CRLs). Proposals leveraging this technique are introduced in our *CAT-I*. Included in *CAT-I* is also a recently proposed pseudonym lookup table (PLT)-based technique [8], which is similar in idea to CRL-based technique with key differences in design and application. *CAT-II* presents a different design rationale using the blocking technique, without reliance on CRLs (and the alike).

2.1. Defense techniques in CAT-I

We have mentioned in Section 1 that handling misbehavior in anonymous VANETs is more challenging and complex since anonymity creates more chances for misbehavior. The discussion of defense techniques hereafter emphasizes on systems providing anonymity.

2.1.1. CRL-based revocation by TA

While traditional certificate revocation techniques such as certificate revocation list (CRL), certificate revocation system (CRS), certificate revocation tree (CRT), etc. in wired networks [10] fail to meet the specifics of vehicular networks, Raya et al. [3] proposed three credential revocation protocols tailored for VANETs, considering that the CRL is generally large in size and the vehicle has limited storage space. Moreover, the CRL needs to be distributed across the entire network in a timely manner.

The first protocol, namely RTPD (Revocation Protocol of the Tamper-Proof Device), is to revoke the tamper-proof device (TPD) equipped in each vehicle. When a revocation decision is made, the TA sends a revocation message encrypted with the target vehicle's public key. The TPD of the vehicle upon receiving and decrypting the message will erase all the stored keys which prevents the vehicle from signing any more messages. Since it renders the vehicle unable to authenticate to others, the messages sent will be ignored by all potential receivers. This protocol will rely largely on infrastructure because the revocation messages have to be sent through base stations. It also requires the TA to acquire or estimate the current location of the vehicle which involves multicast or broadcast via base stations or low-speed FM radio. RTPD is used only when all the keys of the misbehaving vehicle have to be revoked since partial revocation of keys cannot be supported. Furthermore, locating the vehicle to ensure revocation message delivery needs to be highly feasible.

When partial revocation of keys is desired or locating a vehicle is infeasible, RC^2RL (Revocation protocol using Compressed Certificate Revocation Lists) can be employed. This protocol is based on traditional CRL approach with modifications to obtain higher efficiency by means of a lossy compression technique, reducing the communication and storage overhead as well as keeping false revocation rate in a configurable range.

Since RTPD and RC^2RL both rely on pervasive infrastructure, DRP (Distributed Revocation Protocol) is proposed which is used in ad hoc mode before any infrastructure points become available. In this protocol, neighboring vehicles accumulate accusations against misbehaving vehicles by using some technique of detecting malicious data. Once an infrastructure point is reached, neighbors will report accusations to the TA who will then update and distribute the CRL. Note that it is still the TA who manages and distributes the CRL. Neighbors in DRP locally revoke the misbehaving vehicles in order to minimize the damage caused by these vehicles. Due to the additional mechanism employed by neighboring vehicles, the details of which are recently proposed in [11,12], and the unavailability of infrastructure, final distribution of the CRL to the network may not be in time. Nevertheless, this approach is reasonable since the misbehaving vehicle will have the highest impact within its vicinity, and thus the delay of CRL distribution may be tolerated to some extent.

All the three protocols seem to work well under conventional public key infrastructure (PKI). However, the authors in [3] later proposed to use anonymous public keys to achieve anonymity and fulfill the users' requirement on identity and location privacy, where the anonymous public keys are updated frequently enough for the desired level of anonymity. If this privacy preserving technique is used in conjunction with RC^2RL and DRP, the CRL produced by the TA will become huge in size since each vehicle is associated with many anonymous public keys and revoking a vehicle requires revoking all its anonymous keys, rendering the revocation protocols highly inefficient.

2.1.2. CRL-based revocation by access point

Another credential revocation technique is an indirect approach via the aid of an access point, or infrastructure point (i.e., RSUs in [13,9] and base stations in [14]). The TA distributes the CRL to these infrastructure points which then take over the TA's responsibility to execute the revocation protocol. In case the infrastructure points are physically unreachable or are blocked intentionally by misbehaving users, message receivers locally verify the freshness of an infrastructure point's signature on a message sender's certificate and decide if such a freshness is trustworthy. This requires each vehicle to obtain a new signature from an infrastructure point on a periodic base or whenever possible. The advantage of this approach is that vehicles never need to download the entire CRL. Instead, they will be informed by the infrastructure points about a revoked vehicle. Unlike the problem of applying the CRL-based revocation protocols to the anonymous system in [3], the indirect revocation approach cooperates well with the anonymity preserving mechanisms in the above proposals. Specifically, group signature and pseudonym techniques are used in [9,14], respectively, to fulfill conditional anonymity, that is, users' anonymity is guaranteed as long as they do not misbehave. Once misbehaving, the system will be able to reveal the identity of the misbehaving user. Unfortunately, the conditional anonymity claimed in

[9,14] only applies to amongst peer vehicles, under the assumption that the group manager (in [9]) and base station (in [14]) are trusted, since these entities can reveal the identity of any vehicle at any time, regardless of the vehicle being compliant or misbehaving.

2.1.3. PLT-based revocation

A pseudonym lookup table (PLT) is proposed in [8] similar in idea to CRL. The key differences are two folds. First and foremost, the PLT is created and managed at the TA to record the correspondence of a registered vehicle's real identity and pseudonyms [8]. It will not be distributed across the system but rather serves as a central database for online lookup. Another difference is that [8] adopts ID-based PKI instead of conventional PKI and thus pseudonyms can be authenticated alone without the requirement of certificates. Furthermore, authentication can be performed on-the-fly with no exchange of certificates between the two communicating vehicles. It greatly reduces the communication and storage overhead. The revocation technique in [8] was developed to suit the application scenario where the authorities (e.g., policy, judge, trusted network authorities) need to pursue the misbehaving user hiding behind a pseudonym, for liability reasons. While in all previous mentioned proposals in *CAT-I*, the authors deal with the scenario where peer vehicles are the primary potential victims who need to be aware of a misbehaving peer in the network. Different from [9,14], conditional anonymity in terms of both recovering the identity of misbehaving vehicles and maintaining anonymity for compliant vehicles is fulfilled in [8], by using secret sharing technique which eliminates possible abuse to a compliant vehicle from a single authority (assuming at least one cooperating authority is not corrupted). The only complication of the pseudonym revocation technique may be the reliance on available wireless infrastructures (e.g., Wi-Fi, Wireless Mesh Networks, Wireless Ad Hoc Networks) which would require the compatibility and proper interfacing of the vehicle's on-board unit (OBU) to such networks, due to the combinational use of pseudonym preloading (as in [3]) and short-lived pseudonym replenishing (as in [14]) to yield a reasonable sized PLT.

2.2. Defense techniques in CAT-II

Recently, Tsang et al. [15] proposed a blacklistable anonymous credential system for blocking misbehavior without the TTP (Trusted Third Party). The authors claim that the capability of a TTP (or TA in our paper) to recover a user's identity in any case is too strong a punishment and highly undesirable in some applications where users can publish their viewpoints and speech out fearless of being persecuted. Alternatively, the service provider can simply block misbehaving users by his own judgment and hence restricting these users from accessing the provided service. All users in the system, misbehaving or well-behaving, will by no means be identified by any entity. Although not proposed specifically for VANETs, the idea of [15] applies to the defense against misbehavior in our *CAT-II*. Indeed, if the level of misbehavior is low, and also allowing the possibility of vehicles to malfunction, being able to reveal the identity of all misbehaving users as the only means of defense is an unreasonable feature and will render anonymity preserving mechanisms useless, especially in VANETs where user population is huge and misbehavior is expected to occur frequently.

By applying the blocking technique proposed in [15] to cope with misbehavior that falls into *CAT-II*, a vehicle needs to prove to the infrastructure point (e.g., network administrator, service provider) or another vehicle that it is not on the blacklist of the current verifier. If the vehicle fails to provide such a proof (i.e., it is on the blacklist of the verifier), the verifier will ignore the messages or requests sent by this vehicle. There is also a mechanism proposed in [15] to remove a user from the blacklist based on some decision procedure. The technique of Zero-Knowledge Proof of Knowledge (ZKPoK) is used such that the verifier learns nothing about the prover (e.g., any identity-related information) except the fact that the prover is not currently blacklisted. In addition, no entity in the system will have sufficient information to trace and identify any user. It is also possible for two entities to share their blacklist entries so that a user cannot misbehave at an arbitrary number of different locations.

The downside of this technique is obviously the lack of capability to trace misbehaving users. As a result, it cannot be applied to scenarios where identifying the source of misbehavior is a must. Since we can employ defense techniques in *CAT-I* to identify the source of misbehavior, the downside of the blocking technique is not a big issue and research along this line will be needed and encouraged.

3. Preliminaries

This section comprises basic introduction to the cryptographic system and primitive 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 and email address, which avoids the use of certificates for public key verification in the conventional PKI. Boneh and Franklin [16] 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) Non-degenerate: $\exists P, Q \in G_1$ such that $e(P, Q) \neq 1$.
(3) Computable: there exists an efficient algorithm to compute $e(P, Q)$, $\forall P, Q \in G_1$.

IBC schemes are used for encryption, authentication, and deriving shared keys 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. 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 [17] 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.

3.3. Notation

The following notations will be used throughout this paper:

- ID_x: the real identity of an entity x.
- PS_x: the pseudonym of x issued by the RTA.
- $\mathscr{SIG}_{\varpi_x}(m\|t)$: the ID-based signature [18] on a message m concatenated with time t using the signer x's private key ϖ_x. The corresponding public key is PS_x.
- $\mathscr{HMAC}_{\pi}(m\|t)$: the keyed-hash message authentication code on a message m concatenated with time t using cryptographic hash functions and the shared secret key π.

4. DRTA: a new defense technique using threshold authentication

We have mentioned that credential revocation is the most common defense against misbehavior in VANET sytems where misbehaving sources should be possible to identify. We have also presented techniques based on CRLs and the blocking technique in Section 2. We are inspired by the other technique suitable for credential revocation recognized in IEEE P1609.2/D2 [19] (besides CRLs), that is, using short-lived certificates automatically revoke keys, thereby avoiding the maintenance and distribution of CRLs. Although short-lived concept is incorporated into the design of the security framework in [14], the revocation protocols still rely on the distribution of CRLs. The major concern of the short-lived certificates (automatic revocation) is that the short period before the expiration of the certificate inevitably creates a vulnerable period where a supposedly revoked user can continue to misbehave. This concern hinders research along this line and renders the automatic revocation less popular than CRLs in the design of credential revocation protocols.

4.1. Overview

We propose DRTA, Dynamic Revocation with Threshold Authentication, a new misbehavior defense technique leveraging the idea of dynamic revocation, to provide a means of limiting the impact of misbehavior by adjusting it to an acceptable level during the vulnerable period existing in the automatic revocation technique. The dynamic revocation protocol is based on the dynamic k-times anonymous authentication [20] which we call a threshold authentication technique, with k the threshold beyond which any additional number of authentication will result in the revocation of the user's privilege and possible recovery of the user's identity. Consider the VANET environment illustrated in Fig. 1, on which we base all our following discussions.

In our system, a trust domain is managed by a regional transportation authority (RTA). Different among countries, this region can be a state, province, etc. Let the RTA be the TA who registers legitimate vehicles into the region and holds the vehicle identities. The RTA maintains a PLT for each registered vehicle in its domain [8]. In addition to the registration in the VANET system, each vehicle or infrastructure point is also required to enroll with the RTA and become a member of the defense system, where the threshold authentication-based defense scheme is employed. However, the RTA does not know the member's private credential pertinent to the defense system, and hence cannot arbitrarily trace members or reveal their identities unless they misbehave (i.e., by authenticating $k+1$ or more times), as opposed to the group manager in group signature schemes.

Upon detecting misbehavior (possibly using some detection technique which is beyond the scope of this paper. Recall that we have explained the detection of misbehavior is orthogonal to the defense against it.), a vehicle (or infrastructure point) will initiate the anonymous authentication protocol by setting up his own access group to become an access group owner. The access group owner can then exercise control on the communicating entities which we call the access group members. The most fundamental control such an owner has over his members is to determine a threshold k indicating the number of times he will authenticate (or communicate with) a particular member. Note that the access group owner can assign different values of k to different access group members. Moreover, the access group setup provides flexibility when the access group owner intends to place extra restrictions on his members besides the threshold k not being exceeded. Specifically, the access group owner can further restrict his members in two ways: a) the owner needs to control the activity duration of a member in addition to the number of times k, and b) the owner decides to revoke a 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 high severity of the member's misbehavior. An example of (a) can be when the owner is a roadside infrastructure point that provides

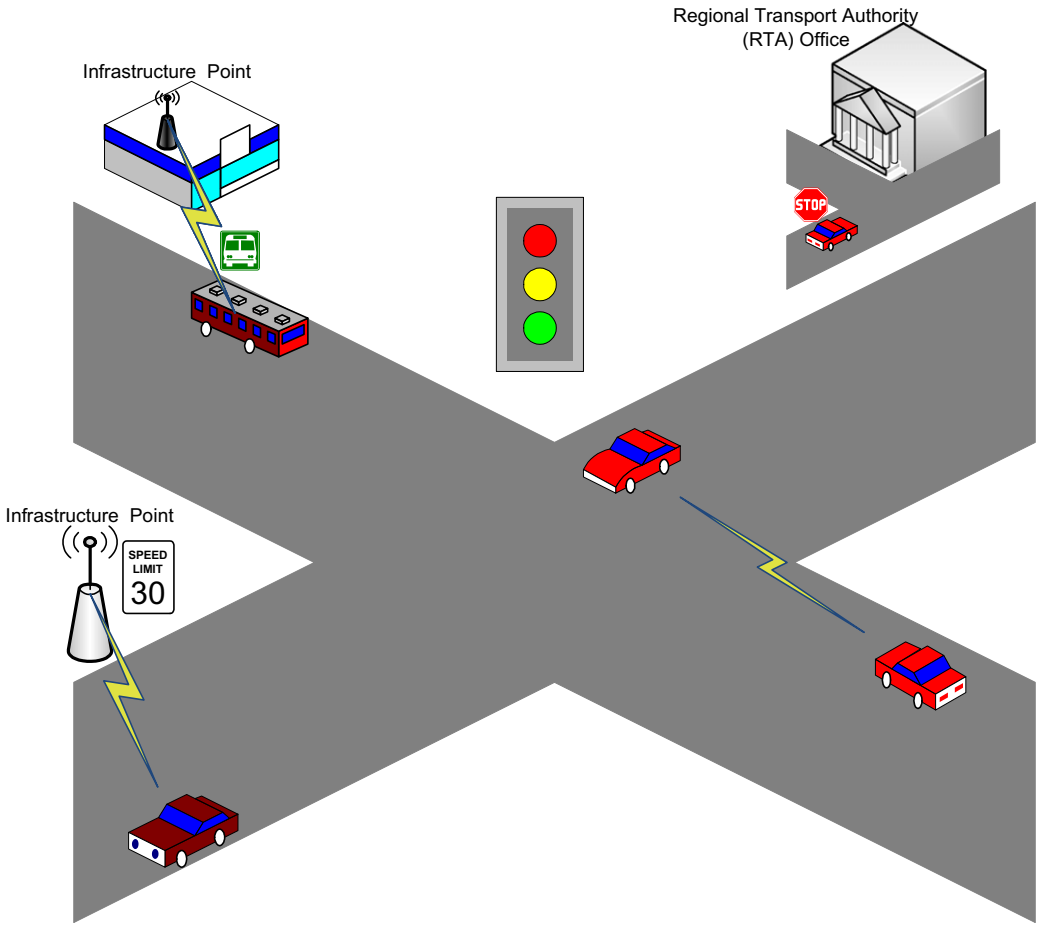


Fig. 1. Our VANET system.

services (e.g., infotainment) bearing an expiration time. In this case, the owner may initiate a timer the first time a member authenticates (using the threshold authentication protocol) and deny the member's access as the timer runs out, even if k has not been reached. In the case of (b), the owner has more control which is necessary when his members include: (1) public vehicles that tend to impact greatly on victims [19] and (2) misbehaving vehicles (that have been detected by the owner) continuing to attack the system during the vulnerable period (i.e., before k is reached, and the certificate has not expired if the automatic revocation technique is being adopted). The access group owner may revoke these members' access as soon as the severity level of their misbehavior goes beyond tolerance (tolerance of misbehavior is design specific and will not be elaborated here). The revocation of a member's access right is realized through the dynamic accumulators proposed in [21] where the revocation cost is independent of the access group size and the revoked user population.

We can see that even if no extra restriction is in place, a malicious access group member can misbehave for at most k times should anonymity be desirable. If the malicious member chooses to authenticate more than k times (remember that authentication has always to be performed before any communications), he automatically surrenders his anonymity since his identity can be recovered in this case. By employing PLT at RTA [8], identification information stored in the identification list ID_{list} (which will later be used by public tracing mechanism as discussed shortly) with pseudonyms or anonymous keys that do not reveal any identity information. Consequently, the result of public tracing mechanism performed when a misbehaving member authenticates himself for more than k times, will return the pseudonym or anonymous key of the misbehaving member who is not identifiable by peer vehicles or infrastructure points running the threshold authentication procedure. In order to trace and identify this member, the RTA will be relied (or we can use secret sharing to separate the role of identity recovering authority). Peer vehicles and infrastructure points can send their accusations to the RTA (i.e., by sending the output pseudonym or anonymous key to the RTA) instead of identifying the misbehaving member themselves, therefore leaving it for the RTA to determine if the accused member should be identified according to the severity of the misbehavior.

4.2. Security objectives

We attempt to achieve the following security objectives:

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.

Traceability: The traceability requirement indicates that a misbehaving user will be identified and the corresponding credential revoked, if necessary, by centralized or distributed approach, to prevent this user from further disrupting system operations.

Non-frameability: Non-frameability requires that no entity in the system can accuse an honest user for being guilty or having misbehaved.

Others: First of all, a secure VANET system should satisfy several fundamental requirements, namely, authentication, message integrity, and confidentiality where sensitive information is being exchanged, to protect the system against unauthorized message injection, message alteration, eavesdropping, respectively.

4.3. The proposed defense scheme

We describe the design details of our defense scheme in the following five procedures.

4.3.1. System setup

Refer to [8] for the initial VANET system setup where a system public/private key pair is assigned to each legitimate user for authentication purpose, before our defense scheme or any other security schemes can be deployed. In general, a VANET user with public/private key pair (PS_v, ϖ_v) broadcasts a message m (e.g., for accident-avoidance, detour notification) as follows:

$$V \rightarrow *: PS_v,\ m,\ \mathscr{SIG}_{\varpi_v}(m\|t),$$

where $\mathscr{SIG}$ denotes the signature scheme for signing message m, and t is the current system time to prevent message replay attack [22]. As mentioned in [8] for preserving user privacy, vehicles always use their pseudonyms as public keys for authentication instead of real identities (cf. Section III.B of [8] for pseudonym generation and update).

On input of 1^κ, the unary representation of the security parameter κ, the key generator outputs a tuple (G_1, G_2, e, P, q) as defined in Section 3.2. 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 identification list ID_{list} which is initially empty and can be accessed by any user of the system.

4.3.2. Enrollment

A user M_n registers with the RTA as follows by first selecting $x',\ r \in_R Z_q^*$:

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

where C' is a commitment that will later be used in ZKP_1. At the end of this protocol, 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 [20] 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 in *Tracing and Revocation* described later in this section.

4.3.3. Access group setup and dynamic revoking

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 $AUTH_{log}$ recording the authentication transcripts, the accumulated value D for dynamically revoking access rights of his access 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. $M_n \rightarrow AGO: PS'_{M_n},\ mpk = (a,S,C,\beta),\ t_5,\ \mathscr{SIG}_{\varpi'_{M_n}}(mpk\|t_5)$;
2. $AGO \rightarrow M_n: PS_{AGO},\ k,\ j,\ D_j,\ t_6,\ \mathscr{SIG}_{\varpi_{AGO}}(k\|j\|D_j\|t_6)$.

Note that we have used PS'_{M_n} here (serving the same purpose as PS_{M_n} in *Enrollment*) 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 access key to $mak = (j+1, W)$ where $W = D_j$, and initiates a running counter d which he compares with the threshold k to ensure that k is not exceeded each time the threshold authentication procedure is executed.

The access group owner revokes M_n's access right when detecting violation to the restriction set on M_n. Such detection 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 as mentioned in Section 3.1. 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.

4.3.4. Threshold authentication

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

$M_n \rightarrow AGO$

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

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 $(\Theta_j, \check{\Theta}_j) = \mathscr{H}_{G_2 \times G_2}(PS_{AGO}, k, j)$ for $j = 1, \cdots, k$. The access group owner aborts the procedure if $d > k$, which ensures that the user cannot authenticate himself more than k times unless he 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 [20] for proof details) to $AUTH_{log}$. 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.

If M_n authenticates with an ordinary user who runs no access group, the access group setup and revoking procedures will be omitted and the threshold authentication procedure will be slightly modified. The ordinary user still obtains a public/private key pair (apk, ask) as in the access group setup procedure, and there will only be the $AUTH_{log}$ but no accumulated value or public archive. M_n will not need to obtain and update the access key mak in the case of an ordinary user. The ordinary user sends his pseudonym in use and the threshold k to M_n for computing tag bases, followed by a same step as the threshold authentication between M_n and the access group owner shown above, except for the proof ZKP_2. M_n need not prove to the ordinary user that he is granted access to some access group since an ordinary user does not set up and manage any access group. M_n only needs to prove to the ordinary user in ZKP_2 that he is a registered member of the VANET system with valid mpk and msk, and he has not authenticated with the ordinary for more than k times. The remaining operations for the ordinary user will be the same as for the access group owner. However, an ordinary user will not be able to exercise control under high level scrutiny due to the lack of his own access group, resulting in higher risks of severe misbehavior or continuing attacks during vulnerable period. Therefore, users in our VANET system are encouraged to setup and manage their own access groups.

4.3.5. Tracing and revocation

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 $\beta = \left(\frac{\check{\Gamma}}{\check{\Gamma}'}\right)^{\overline{l-l'}} = A^x$. 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.

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 [8] 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. Analysis and comparison

The performance of our defense scheme is evaluated in comparison with existing schemes.

5.1. Analysis of the proposed scheme

Analysis is carried out in terms of security, and efficiency including storage, computation, and communication efficiencies.

5.1.1. Security

Our security analysis is in regard to the security requirements for VANETs specified in Section 1.1. In the proposed VANET system, authentication and data integrity are guaranteed by ID-based signatures, as shown in Section 3. If a shared secret key is established between communicating entities, data integrity can be protected with the message authentication code (e.g., $\mathscr{HMAC}$). Confidentiality which is not shown in our scheme can be attained by using public or symmetric key encryptions, for the initial and subsequent secure communications, respectively. The adoption of pseudonyms in VANET communications conceals the real identity of vehicles such that peer vehicles and infrastructure access points cannot identify the sender of a specific message while are still able to authenticate the sender. By frequently updating the pseudonyms during communications (cf. Section 3. B in [8]) via anonymous substrate such as [23,24], our system defends legitimate vehicles against location tracing and user profiling. The tracing protocol in the threshold authentication scheme guarantees the traceability of a misbehaving user who is restricted to authenticate no more than k times but has exceeded this threshold. Note that it is not possible for any entity in the system to frame an honest user simply because an evidence (i.e., authentication transcripts) cannot be produced for verification by the authority, thereby

assuring non-frameability. Other requirements pertinent to VANET security include data consistency, availability, position verification, efficiency, and scalability, and are discussed in [25,26,5,27,28,1], respectively. These requirements are not the security goals of our VANET system but can be fulfilled by applying the above techniques accordingly.

5.1.2. Efficiency

Storage: In our system, the storage requirements on RTAs and infrastructure points 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. We adopt the parameters specified in [29] 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 needs to store a public/private key pair, roughly 214 bytes, for the ID-based defense scheme. 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 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. 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 [8]. The 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.

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 signatures and shared keys when exchanging messages with other vehicles. ID-based signature schemes such as [18] can be utilized for the signing and verification procedures. Using the techniques in [18], computation efficiency can be achieved by pre-computing 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. The vehicle also needs to compute pairings for the defense scheme, where the zero-knowledge proof (ZPK) construction and verification contribute to the highest cost since they must be performed each time an access group owner authenticates an access group member. The proofs can be constructed by access group members in advance and hence all pairings involved can be pre-computed. In contrast, certain number of pairings must be computed in real-time while others can be pre-computed for the verification performed by the access group owner. Employing the construction and verification shown in [20], four pairings need be computed by the access group owner in real-time. Some pairing operations involved in *Enrollment* and *Access Group Setup and Dynamic Revoking* can be neglected due to the infrequent invocation of these procedures.

Although the computationally intensive pairing operations are not involved in conventional 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 [30] 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 1024-bit RSA while the last field has effective 922-bit security. Recent progress [31] 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. Moreover, recent results show the feasibility of pairings on power-constrained smartcards [32,33], which we believe strengthens our 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.

Communication: Communication costs in our systems are mainly induced by broadcasts. Each message broadcasted by vehicles (cf. Section 3.1) consists of a pseudonym (22 bytes), a plaintext message (disregarded in the comparisons) and a signature. The signature generated by the scheme in [18] 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 1.1KBytes communication overhead (assuming the RSA key for signing is 1024-bit or 128-byte, and a standard certificate comprising an RSA public key and the certificate authority's signature is roughly 1 KBytes). Apparently, our ID-based solution outperforms ECC-based PKI and has significant improvement compared to RSA-based PKI. Analogous to the broadcast of messages, the broadcast occurred during *Tracing and Revocation* in the defense scheme, introducing roughly 1.2 Kbytes, also takes place only in a vehicle's transmission range. As described in Section 3.3, 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 Kbytes) for verification purpose need not be broadcasted.

Table 1
A comparison of defense techniques against misbehavior in anonymous VANETs – part I.

	Defense technique
RTPD [3]	Revocation of TPD
RC^2CL [3]	Compressed CRL
DRP [11]	Locally revoke first by neighbors, then CRL by TA
GSIS [9]	CRL to RSUs only, who take over revocation from TA
Kamat [14]	CRL to BSs only, who take over revocation from TA
Sun [8]	PLT similar to CRL
Tsang [15]	Blacklist without identifiability
DRTA	Short-lived certificates by TA

Table 2
A comparison of defense techniques against misbehavior in anonymous VANETs – part II.

	Cond. anonymity – AS1	Cond. anonymity – AS2
RTPD [3]	Yes, anonymous keys	Yes, secret sharing
RC^2CL [3]	Same as above	Same as above
DRP [11]	Same as above	Same as above
GSIS [9]	Yes, group signatures	No
Kamat [14]	Yes, pseudonyms	No
Sun [8]	Yes, pseudonyms	Yes, secret sharing
Tsang [15]	No, full anonymity	No, full anonymity
DRTA	Yes, anonymous credentials	Yes, threshold authentication

Table 3
A comparison of defense techniques against misbehavior in anonymous VANETs – part III.

	Limitation
RTPD [3]	All keys have to be revoked once TPD must be reachable
RC^2CL [3]	heavy reliance on infrastructure Added complexity to CRLs
DRP [11]	Data detection mechanism adds complexity It may render CRLs not in time
GSIS [9]	GM can always reveal any ID Reliance on infrastructure Revocation only within vicinity
Kamat [14]	Heavy reliance on infrastructure Revocation creates vulnerable period Revocation only within vicinity
Sun [8]	Reliance on other wireless networks Compatibility and interfacing of OBUs to such networks
Tsang [15]	Misbehaving users are not identifiable in any case Not desirable for systems with liability concerns
DRTA	Reliance on other wireless networks Compatibility and interfacing of OBUs to such networks Neighbor sharing for best performance but incurs comm. overhead

5.2. Comparisons of different defense schemes

Comparisons of the defense techniques introduced in this paper is given in Tables 1–3. Important aspects of these proposals are summarized for improved readability. Note that we separate conditional anonymity into two aspects: Cond. Anonymity – AS1 denotes the aspect that the system is capable of tracing and identifying misbehaving users, and Cond. Anonymity – AS2 denotes the aspect that compliant users are not traceable or identifiable by any entities unless misbehavior occurs which serves as a trigger for traceability and identifiability.

6. Conclusion

Misbehavior is expected to occur frequently in VANETs due to a large user base. Defense against misbehavior under different system requirements are critical to mitigate the impact of misbehaving users on the network. This paper first reviews the commonly adopted defense techniques based on the classification of misbehavior types in anonymous VANETs where anonymity adds complication to defense techniques against misbehavior. We then present our proposed defense scheme DRTA (Dynamic Revocation using Threshold Authentication) and show that the scheme is secure, highly flexible and dynamic in defending anonymous VANET systems against various possible types of misbehavior. Through performance evaluation and comparisons with existing schemes, we demonstrate the feasibility and performance gain of DRTA in terms of misbehavior defense in the anonymous VANET system of interest.

Acknowledgements

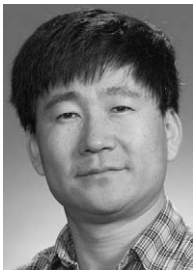
This work was supported in part by the U.S. National Science Foundation under Grants CNS-0721744, CNS-0716450, CNS-0626881 and CNS-0716302.

References

[1] K. Plößl, T. Nowey, C. Mletzko, Towards a security architecture for vehicular ad hoc networks, in: Proc. First Int. Conf. on Availability, Reliability and Security, ARES'06, April 2006.
[2] B. Parno, A. Perrig, Challenges in securing vehicular networks, in: Proc. Fourth Workshop on Hot Topics in Networks, HotNets-IV, November 2005.
[3] M. Raya, J.-P. Hubaux, Securing vehicular ad hoc networks, Journal of Computer Security 15 (1) (2007) 39–68. special issue on Security of Ad Hoc and Sensor Networks.
[4] J.Y. Choi, M. Jakobsson, S. Wetzel, Balancing auditability and privacy in vehicular networks, in: Proc. First ACM Int. Workshop on QoS and Security for Wireless and Mobile Networks, Q2SWinet'05, October 2005, pp. 79–87.
[5] T. Leinmüller, C. Maihöfer, E. Schoch, F. Kargl, Improved security in geographic ad hoc routing through autonomous position verification, in: Proc. Third ACM Int. Workshop on Vehicular Ad Hoc Networks, VANET'06, September 2006.
[6] M.E. Zarki, S. Mehrotra, G. Tsudik, N. Venkatasubramanian, Security issues in a future vehicular network, in: Proc. European Wireless 2002, February 2002.
[7] M. Raya, J.P. Hubaux, Security aspects of inter-vehicle communications, in: Proc. Swiss Transport Research Conference, STRC, March 2005.
[8] J. Sun, C. Zhang, Y. Fang, An id-based framework achieving privacy and non-repudiation in vehicular ad hoc networks, in: Proc. IEEE Military Communications Conf., October, 2007, pp. 1–7.

[9] X. Lin, X. Sun, P.-H. Ho, X. Shen, GSIS: a secure and privacy-preserving protocol for vehicular communications, IEEE Trans. Vehicular Tech. 56 (6) (2007) 3442–3456.
[10] P. Zheng, Tradeoffs in certificate revocation schemes, SIGCOMM, Computing Communication Review 33 (2) (2003) 103–112.
[11] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, J.-P. Hubaux, Eviction of misbehaving and faulty nodes in vehicular networks, IEEE J. Select. Areas Communications 25 (8) (2007).
[12] M. Raya, M.H. Manshaei, M. Félegyházi, J.-P. Hubaux, Revocation games in ephemeral networks, in: ACM Conference on Computer and Communications Security, October 2008.
[13] X. Lin et al., Security in vehicular ad hoc networks, IEEE Communications Magazine 46 (4) (2008) 88–95.
[14] P. Kamat, A. Baliga, W. Trappe, An identity-based security framework for VANETs, in Proc. Third ACM Int. Workshop on Vehicular Ad Hoc Networks, VANET'06, pp. 94–95, September 2006.
[15] P. Tsang, M.H. Au, A. Kapadia, S.W. Smith, Blacklistable anonymous credentials: Blocking misbehaving users without TTPs, in: ACM Conference on Computer and Communications Security, 2007, pp. 72–81.
[16] D. Boneh, M. Franklin, Identity-based encryption from the weil pairings, in: Advances in Cryptology – Asiacrypt 2001, LNCS, vol. 2248, Springer-Verlag, 2001, pp. 514–532.
[17] C.-P. Schnorr, Efficient signature generation by smart cards, J. Cryptol 4 (3) (1991) 161–174.
[18] F. Hess, Efficient identity-based signature schemes based on pairings, SAC 2002, LNCS, vol. 2595, Springer-Verlag, 2002, pp. 310–324.
[19] IEEE Std 1609.2-2006, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages, 2006. <http://ieeexplore.ieee.org/servlet/opac?punumber=11000>.
[20] L. Nguyen, R. Safavi-Naini, Dynamic *k*-times anonymous authentication 3531 (2005) 318–333.
[21] J. Camenisch, A. Lysyanskaya, Dynamic accumulators and application to efficient revocation of anonymous credentials, in: CRYPTO 2002, LNCS, vol. 2442, Springer-Verlag, 2002, pp. 61–76.
[22] A. Menezes, P.V. Oorschot, S. Vanston, Handbook of Applied Cryptography, CRC Press, Boca Raton, 1996.
[23] R. Dingledine, N. Mathewson, P. Syverson, Tor: the second-generation onion router, in: Proc. The 13th USENIX Security Symposium, August 2004, pp. 303–320.
[24] R. Dingledine, Tor: an anonymous internet communication system, in: Workshop on Vanishing Anonymity, The 15th Conf. on Computers, Freedom, and Privacy, April 2005.
[25] P. Golle, D. Greene, J. Staddon, Detecting and correcting malicious data in VANETs, in: Proc. First ACM Int. Workshop on Vehicular Ad Hoc Networks, VANET'04, October 2004, pp. 29–37.
[26] J. Yin, T. Elbatt, G. Yeung, B. Ryu, S. Habermas, H. Krishnan, T. Talty, Performance evaluation of safety applications over DSRC vehicular ad hoc networks, in: Proc. First ACM Int. Workshop on Vehicular Ad Hoc Networks, VANET'04, October 2004.
[27] T. Leinmüller, E. Schoch, F. Kargl, Position verification approaches for vehicular ad hoc networks, IEEE Wireless Communications October (2006) 16–21.
[28] M. Raya, A. Aziz, J.P. Hubaux, Efficient secure aggregation in VANETs, in Proc. Third ACM Int. Workshop on Vehicular Ad Hoc Networks, VANET'06, September 2006, pp. 67–75.
[29] J. Sun, C. Zhang, Y. Fang, A security architecture achieving anonymity and traceability in wireless mesh networks, in: IEEE Conf. on Computer Communications (INFOCOM), April 2008, pp. 1687–1695.
[30] P.S.L.M. Barreto, H.Y. Kim, B. Lynn, M. Scott, Efficient algorithms for pairing-based cryptosystems, in: CRYPTO 2002, LNCS, vol. 2442, Springer-Verlag, 2002, pp. 354–368.
[31] P.S.L.M. Barreto, S.D. Galbraith, C. ÓhÉigeartaigh, M. Scott, Efficient pairing computation on supersingular abelian varieties, Cryptology ePrint Archive, Report 2004/375, September 2005. Available at <http://eprint.iacr.org/2004/375.pdf>.
[32] M. Scott, N. Costigan, W. Abdulwahab, Implementing cryptographic pairings on smartcards, in: L. Goubin, M. Matsui, CHES 2006, LNCS, vol. 4249, Springer-Verlag, 2006.
[33] G.M. Bertoni, L. Chen, P. Fragneto, K.A. Harrison, G. Pelosi, Computing tate pairing on smartcards, 2005. <http://www.st.com/stonline/products/families/smartcard/ches2005_v4.pdf>.

Jinyuan Sun received the M.A.Sc. degree in computer networks from Ryerson University, Canada, in 2005. She received the B.S. degree in computer information systems from Beijing Information Technology Institute, China, in 2003. She was a Network Test Developer at RuggedCom Inc., Ontario, Canada, 2005–2006. She is currently working towards the Ph.D. degree in the University of Florida. Her research interests are in the security protocol and architecture design of wireless networks. She is a student member of the IEEE.



Yuguang Fang received a Ph.D. degree in Systems Engineering from Case Western Reserve University in January 1994 and a Ph.D. 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 University of Florida in May 2000 as an assistant professor, got an early promotion to an associate professor with tenure in August 2003 and a professor in August 2005. He has published over 150 papers in refereed professional journals and conferences. He received the National Science Foundation Faculty Early Career Award in 2001 and the Office of Naval Research Young Investigator Award in 2002. He has served on many editorial boards of technical journals including IEEE Transactions on Communications, IEEE Transactions on Wireless Communications, IEEE Transactions on Mobile Computing and ACM Wireless Networks. He is a fellow of the IEEE.