A DEFENSE TECHNIQUE AGAINST MISBEHAVIOR IN VANETs BASED ON THRESHOLD AUTHENTICATION

Jinyuan Sun and Yuguang Fang
University of Florida, Gainesville, FL

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 propose a defense technique to handle misbehavior in VANETs, caused by either malfunctioning hardware (unintentional) or purposeful attacks. It can be used in both inter-vehicle and vehicle-to-infrastructure communications, where user privacy is highly desirable but adds more complexity to the defense. By employing our misbehavior defense technique, users of the system can opt for allowing occasional or unintentional misbehavior while preventing frequent or disruptive misbehavior.

I. INTRODUCTION

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. On the contrary, misbehavior of legitimate users (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 base stations that can be easily tricked into trusting the insiders. Consequently, the insiders' misbehavior will have much larger impact on the network and be more devastating. Recently most proposals on VANET security [1], [2], [3] 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 and thus is the focus of our work to handle misbehavior in VANETs relying on anonymous communications, since user identity is hidden and cannot be linked arbitrarily which curbs the punishment of misbehaving users.

978-1-4244-2677-5/08/$25.00

It is stressed that we are interested in the defense technique against misbehavior that 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 attacks 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 [1].

A. RELATED WORK

The existing defense techniques against misbehavior in VANET literature, which are of interest in this paper, fall into one of the following two categories.

a) In the first category, the misbehaving user must be identified by the trusted authority (TA) and the credential will be revoked correspondingly. This is especially desired in VANETs where liability is a concern. For instance, law enforcement departments require the vehicle identity to be recovered for investigating the cause of accidents or crimes. The requirement of revealing identities implies that the privacy protection provided in VANETs should be *conditional* since otherwise a misbehaving user's identity is no longer traceable. Other TAs (except law enforcing authority) may require identity recovery for punishing misbehaving vehicles of VANETs depending on the severity of the misbehavior and the policy for handling misbehavior implemented

at the TAs. 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 commonly used technique for credential revocation is through the update and distribution of the certificate revocation list (CRL), which is created based on various misbehavior detection mechanisms.

Raya $et\ al.$ [1] proposed three credential revocation protocols tailored for VANETs, namely RTPD, RC^2RL, and DRP, considering that the 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 TA will become huge in size rendering the revocation protocols highly inefficient.

An indirect approach via the aid of infrastructure is used in [3] and [4]. 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. Instead, they will be informed by the infrastructure points about a revoked vehicle. The indirect revocation approach cooperates well with the anonymity preserving mechanisms in these proposals. Unfortunately, the conditional anonymity claimed in [3] and [4] only applies to amongst peer vehicles, under the assumption that the infrastructure points (group manager in [3] and base station in [4]) are trusted, since these entities can reveal the identity of any vehicle at any time, regardless of the vehicle being honest or misbehaving.

A pseudonym lookup table (PLT) is proposed in [2] which is similar in idea to the CRL. The difference is that [2] adopts ID-based PKI instead of conventional PKI and thus pseudonyms can be authenticated alone without the requirement of certificates. The revocation technique considered in [2] mainly suits the authorities (e.g., policy, judge, trusted network authorities) to pursue the misbehaving user hiding behind the pseudonym for liability reasons, while in all previous mentioned proposals, the authors deal with the scenario where peer vehicles or infrastructure points need to be aware of a misbehaving vehicle in the network. Conditional anonymity in terms of both recovering the identity of misbehaving vehicles and maintaining anonymity for honest vehicles can be guaranteed in [2].

b) On the other hand, some type 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. Identity recovery 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 coping with misbehaving users based on an individual's own discretion yields flexibility and dynamics in VANET design.

Recently, Tsang $et\ al.$ [5] proposed a blacklistable anonymous credential system for blocking misbehavior without the trusted third party (TTP). Although not proposed specifically for VANETs, the authors of [5] have a similar claim as ours 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 content fearless of being persecuted. Therefore, the blocking technique of [5] can be applied in VANETs as: if the vehicle fails to prove that he is not on the blacklist of the current verifier, the verifier will ignore the messages or requests sent by this vehicle. Any user in the system, misbehaving or well-behaving, will by no means be identified by any other entity (the TA, infrastructure points, or peer vehicles). The downside of this technique is obviously the lack of capability to trace misbehaving users when necessary, rendering this technique only desirable for certain application scenarios such as those considered in [5].

B. OUR CONTRIBUTIONS

Our work is based on the following observations.
1) We have presented defense techniques mainly based on CRLs in Section I.A for credential revocation. There is another suitable technique for credential revocation recognized in IEEE P1609.2/D2 [6], that is, using short-lived certificates automatically revoke credentials, thereby avoiding the maintenance and distribution of CRLs. These two techniques share a common feature that some entity in the system is able to recover the misbehaving user's identity somehow, as opposed to the defense technique proposed by [5]. Although short-lived concept is incorporated into the design of the security

framework in [4], the revocation protocols still rely on the distribution of CRLs. The major concern of the short-lived certificates (to be used interchangeably with automatic revocation) is the existence of the vulnerable period, the short duration before the expiry of the certificate, in which a supposedly revoked user can continue to misbehave. This concern along with the unavailability of infrastructure hinders research on the automatic revocation technique and renders this technique less popular than CRLs in the design of credential revocation schemes.

2) We have agreed on the claim in [5] that identity recovery is over stringent to some types of misbehavior (cf. Section I.A) which should be allowed and tolerated to some extent that will not create disruption or severe impact on system operations (as to what extent is based on individual judgements). However, the approach used in [5] goes to the other extreme where the identity cannot be recovered by anyone at any time, and thus is inappropriate for VANET systems involving liability issues.

As a result, we propose a new misbehavior defense scheme based on threshold authentication technique [7] to provide a means of: 1) limiting the impact of misbehavior during the vulnerable period (if automatic revocation is used) by setting a threshold on the number of times a suspected or misbehaving user can authenticate himself, and 2) allowing accidental misbehavior (e.g., malfunctioning hardware) and occasional trivial misbehavior (that says, everyone makes mistakes once in a while). The threshold authentication technique yields dynamics and flexibility in each user's setting of threshold on other users being authenticated. It also guarantees that any additional authentication beyond the threshold will result in the traceability of the misbehaving user's credential (different from the user's real identity, cf. Section III.A) and the possible identity recovery by the authority. Moreover, the dynamic accumulators adopted by the threshold authentication technique in [7] renders it more flexible for each user to set up his own access group and revoke group members' access rights, enabling each user to place further restrictions (besides the threshold) on other communicating users. This feature will be most attractive to service providers as discussed in Section IV.A.

However, it is important to notice that our scheme is different from the original threshold authentication scheme in [8] and other variations [7], [9], in that our scheme does not allow any entity to publicly recover the misbehaving user's identity but to leverage the authority for identity recovery, if necessary. The reason is that our scheme is tailored for VANET system where peer vehicles and roadside infrastructure points are not authorized to revoke a credential or recover an identity.

The rest of this paper is organized as follows. Section II introduces some preliminaries relevant to our work. Section III describes the system model including the entities and protocols involved in our scheme, and the security requirements. Section IV elaborates on the proposed defense scheme using threshold authentication technique. Discussion on the fulfillment of security goals is presented in Section V and Section VI concludes the paper.

II. PRELIMINARIES

A. BILINEAR PAIRING

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 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 $e(P, Q), \forall P, Q \in G_1$.

B. 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 [10] 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.

III. SYSTEM MODEL

We describe the entities and the protocols executed in this section for our VANET system. The security requirements of the system will also be presented.

A. ENTITIES AND PROTOCOLS

The entities in our system are the regional transportation authority (RTA), infrastructure access points (IAP), and vehicles (V_i's). These entities are involved in the following protocols: system setup, registration, access group (AG) setup, AG revoking, threshold authentication, tracing, and revocation/recovery.

System setup This protocol is executed by the RTA for initial VANET system setup. On input of a security parameter, the protocol outputs a group public and private key, gpk and gsk, respectively. The RTA publishes gpk and keeps gsk confidential.

Registration Each legitimate user, IAP or V_i registers with the RTA to use the features offered by the VANET system. Upon successful registration, a member public/private key pair (mpk, msk) is issued to an IAP or V_i. The RTA associates the member's credential with the issued public key and includes this pair of information into an credential list ID_{list}.

AG setup Legitimate users of the VANET system can choose to setup their own access groups, the member of which is granted privilege to communicate with the AG owner (AGO). The AGO adds members to the access group and updates related public information. Each added member obtains an AG access key mak. We will discussion in Section IV.A that this protocol is not mandatory for all users in the system.

AG revoking The AGO revokes the granted privilege when he decides to stop communications with a member, due to some decision criteria (cf. Section IV.A). The AGO removes the member from his AG and updates related public information. Note that *AG setup* and *AG revoking* appear in pairs.

Threshold authentication This protocol is executed between an IAP and a vehicle, or between peer vehicles. We call the authenticator in this protocol AU 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 authenticating with the AU is a registered member of the VANET system, this user is a legitimate member of the AU's access group (if the AU is an AGO) whose member privilege has not been revoked, and the authentication threshold has not been exceeded. The AU records the authentication transcripts in $AUTH_{log}$.

Tracing This protocol is used by the AU to trace a misbehaving member M_n who attempts to authenticate more than k times. The AU relies on the $AUTH_{log}$ and public information, and obtains M_n's credential n as the protocol 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 recovered. The RTA performs the recovery by looking up the PLT which records the correspondence between the credential n and identity ID_n.

B. SECURITY REQUIREMENTS

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.

Furthermore, privacy, traceability, and non-frameability are required for our specific VANET system. The privacy requirement states that private information such as vehicle owner's identity and location privacy is preserved against unlawful tracing and user profiling, since otherwise it is difficult to attract vehicles to join in the network. The traceability requirement indicates that a misbehaving user will be identified and the corresponding credential revoked to prevent him from further disrupting system operations. As elaborated in Section IV, certain criteria have to be met for the traceability of a misbehaving user in our system. Non-frameability requires that no entity in the system can accuse an honest user for having misbehaved.

IV. THRESHOLD AUTHENTICATION BASED DEFENSE SCHEME

We give overview of our scheme in this section and the notation used for describing the technical details.

A. OVERVIEW

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. Refer to Section III.A in [2] 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, $\mathcal{SIG}_{\varpi_v}(m \parallel t)$,

where $\mathcal{SIG}$ denotes the signature scheme for signing message m, and t is the current system time to prevent message replay attack [11]. As mentioned in [2] for preserving user privacy, vehicles always use their pseudonyms as public keys for authentication instead of

real identities (cf. Section III.B of [2] for pseudonym generation and update).

Furthermore, the RTA maintains a PLT for each registered vehicle in its domain [2]. After the initial system setup, each legitimate user is required to register with the RTA and become a member of the defense system, where the threshold authentication based defense scheme is employed. Though a member can choose not to run our defense scheme and instead select any defense method mentioned in Section I.A, other members who run our defense scheme will require the membership of their communicating parties. The AG setup and revoking protocols in the defense scheme remain optional and will be incorporated when the AGO intends to place extra restriction on his AG members besides the threshold k not being exceeded. Specifically, the AGO restricts his AG members in two cases: a) the AGO needs to control the activity duration of an AG member in addition to the number of times k, and b) the AGO decides to revoke an AG 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 AGO is a roadside IAP who provides services (e.g., infotainment) bearing an expiration time. In this case, the AGO may initiate a timer the first time an AG 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 AGO has more control over AG members such as public vehicles that tend to impact greatly on victims [6], and misbehaving vehicles (that have been detected by the AGO) continuing to attack the system during the vulnerable period. The AGO may revoke these members' access as soon as the severity level of their misbehavior goes beyond the AGO's tolerance (the tolerance of misbehavior is a design specific and will not be elaborated here). The revocation of an AG member's access right is realized through the dynamic accumulators proposed in [12] where the revocation cost is independent of the access group size and the revoked user population.

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.
- $\mathcal{SIG}_{\varpi_x}(m \parallel t)$: the ID-based signature [13] on a message m concatenated with time t using the signer x's private key ϖ_x. The corresponding public key is PS_x.
- $\mathcal{HMAC}_{\pi}(m \parallel t)$: the keyed-hash message authentication code on a message m concatenated with time t using cryptographic hash functions and the shared secret key π.

B. DESCRIPTION

1) SYSTEM SETUP: On input of a security parameter 1^{κ}, the protocol outputs a tuple (G_1,G_2,e,P,q) as defined in Section II.A. 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} (cf. Section III.A) which is initially empty and can be accessed by any user of the system.

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

1. $M_n \rightarrow RTA$: $PS_{M_n}, C' = x'P + rH, t_1$, $\mathcal{HMAC}_{\pi}(C' \parallel t_1)$;
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 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 [7] 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.

3) AG SETUP: A user opting for his own AG to place further restriction on other users acts as an AGO. The AGO 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 AGO maintains the following information: the $AUTH_{log}$ (cf. Section III.A), the accumulated value D for automatically revoking access rights of his AG members, and a public archive

ARC of the form (a, b, D) where $b = 1, 0$ indicates the grant, revocation of an AG member, respectively. Initially, D is set to $D_0 \in G_1$, $AUTH_{log}$ and ARC are empty. A user M_n joins the AGO's group as follows to further communicate with the 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 ***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 AG successfully, the AGO 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 protocol is executed.

4) AG REVOKING: The AGO 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 IV.A. The AGO simply updates the accumulated value to $D_{j+1} = \frac{1}{s+a}D_j$ and adds $(a, 0, D_{j+1})$ to ARC.

5) THRESHOLD AUTHENTICATION: If M_n is an AG member of an 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 $j = 1, \cdots, k$. The AGO aborts the protocol 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 AGO checks if TAG is different from all other entries in $AUTH_{log}$. If different and ZKP_2 is valid, the AGO adds (TAG, l) and the proof of knowledge ZKP_2 (refer to [7] for proof details) to $AUTH_{log}$. If TAG already exists and ZKP_2 is valid, the AGO proceeds to the tracing protocol below to detect the misbehaving user. If ZKP_2 is invalid, M_n is ignored and the protocol is aborted.

If M_n authenticates with a non-AGO user, denoted by BTO, the AG setup and revoking protocols will be omitted and the threshold authentication protocol will be slightly modified: the BTO still obtains a public/private key pair (apk, ask) as in the AG setup protocol, 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 BTO. However, as mentioned in Section IV.A, a BTO will not be able to exercise control under high-level scrutiny due to the lack of his own AG, 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 AGs.

6) 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 AGO 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 AGO 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 AGs (if any). Note that the AGO 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.

7) 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 protocol when a user truly misbehaves. However, this assumption may be too strong in realistic applications where the RTA can be corrupt. We can use a similar method as in [2] 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.

V. SECURITY ANALYSIS

Major security goals of our VANET system are presented in Section III.B. Specifically, authentication and

data integrity are guaranteed by ID-based signatures, as shown in Section IV.B. If a shared secret key is established between communicating entities, data integrity can be protected with the message authentication code (e.g., $\mathcal{HMAC}$). 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 III.B in [2]), 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. The secret sharing technique (cf. Section III.C in [2]) ensures non-frameability in the case of a corrupt authority when a misbehaving user's identity needs to be recovered. Note that it is not possible for any other 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. Other requirements pertinent to VANET security include data consistency, availability, position verification, efficiency, and scalability, and are discussed in [14], [15], [16], [17], [18] and [19], respectively. These requirements are not the security goals of our VANET system but can be fulfilled by applying the above techniques accordingly.

VI. CONCLUSION

Misbehavior is expected to occur frequently in VANETs due to the large user base. Defense against misbehavior under different system requirements are critical to mitigate the impact of misbehaving users on the system. This paper proposes a new misbehavior defense scheme based on threshold authentication which renders automatic revocation (i.e., using short-lived credentials) a feasible credential revocation technique without CRLs, which significantly reduces the communication cost and gives chances to unintentional or occasional misbehavior that should be tolerated.

ACKNOWLEDGMENT

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

REFERENCES

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

[2] J. Sun, C. Zhang, and Y. Fang, "An id-based framework achieving privacy and non-repudiation in vehicular ad hoc networks," *Proc. IEEE Military Communications Conf.*, pp. 1–7, Oct. 2007.

[3] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Vehicular Tech.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[4] P. Kamat, A. Baliga, and W. Trappe, "An identity-based security framework for VANETs," *in Proc. 3rd ACM Int'l Workshop on Vehicular Ad Hoc Networks, VANET'06*, pp. 94–95, Sept. 2006.

[5] P. Tsang, M. H. Au, A. Kapadia, and S. W. Smith, "Blacklistable anonymous credentials: Blocking misbehaving users without TTPs," *in ACM Conference on Computer and Communications Security*, pp. 72–81, 2007.

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

[7] L. Nguyen and R. Safavi-Naini., "Dynamic k-times anonymous authentication," vol. 3531, pp. 318–333, 2005.

[8] I. Teranisi, J. Furukawa, and K. Sako, "k-times anonymous authentication," *ASIACRYPT 2004, Springer-Verlag, LNCS 3329*, pp. 308–322, 2004.

[9] J.W.Mark and S.Zhu, "Power control and rate allocation in multirate wideband CDMA systems," *in Proc. IEEE Wireless Communications and Networking Conf.*, vol. 1, pp. 168–172, Sept. 2000.

[10] C.-P. Schnorr, "Efficient signature generation by smart cards," vol. 4, no. 3, pp. 161–174, Jan. 1991.

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

[12] J. Camenisch and A. Lysyanskaya, "Dynamic accumulators and application to efficient revocation of anonymous credentials," *CRYPTO 2002, Springer-Verlag, LNCS 2442*, pp. 61–76, 2002.

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

[14] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," *in Proc. 1st ACM Int'l Workshop on Vehicular Ad Hoc Networks, VANET'04*, pp. 29–37, Oct. 2004.

[15] 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," *in Proc. 1st ACM Int'l Workshop on Vehicular Ad Hoc Networks, VANET'04*, Oct. 2004.

[16] T. Leinmüller, C. Maihöfer, E. Schoch, and F. Kargl, "Improved security in geographic ad hoc routing through autonomous position verification," *in Proc. 3rd ACM Int'l Workshop on Vehicular Ad Hoc Networks, VANET'06*, Sept. 2006.

[17] T. Leinmüller, E. Schoch, and F. Kargl, "Position verification approaches for vehicular ad hoc networks," *IEEE Wireless Communications*, pp. 16–21, Oct. 2006.

[18] M. Raya, A. Aziz, and J. P. Hubaux, "Efficient secure aggregation in VANETs," *in Proc. 3rd ACM Int'l Workshop on Vehicular Ad Hoc Networks, VANET'06*, pp. 67–75, Sept. 2006.

[19] K. Plößl, T. Nowey, and C. Mletzko, "Towards a security architecture for vehicular ad hoc networks," *in Proc. 1st Int'l Conf. on Availability, Reliability and Security, ARES'06*, Apr. 2006.