EFFICIENT AND DYNAMIC GROUPING SCHEME WITH SECURE AUTHENTICATION FOR VANET

Gisna Baby[1] | Ms R.Sujitha[2]
[1](UG Student, Christ the King Engineering College)
[2](Assistant Professor, Christ the King Engineering College, srisuji14@gmail.com)

Abstract— *Data congestion control is an efficient way to decrease packet loss and delay and increase the reliability of VANETs. In this paper, a centralized and localized data congestion control strategy is proposed to control data congestion using roadside units (RSUs) at intersections. The proposed strategy consists of three units for detecting congestion, clustering messages, and controlling data congestion. In this strategy, the channel usage level is measured to detect data congestion in the channels. The messages are gathered, filtered, and then clustered by machine learning algorithms. K- means algorithm clusters the messages based on message size, validity of messages, and type of messages. The data congestion control unit determines appropriate values of transmission range and rate, contention window size, and arbitration inter frame spacing for each cluster.*

Keywords—Data Compression, Privacy, Protocol Design, Security, Vehicular Ad Hoc Networks (VANETs)

1. INTRODUCTION

VEHICULAR ad hoc networks (VANETs) have attracted substantial attention in both industry and academia [1]–[5]. A VANET typically consists of vehicles and properly distributed roadside units (RSUs). A vehicle can send/receive safety-related messages (e.g., speed, location, dangerous road Manuscript received October 17, 2014; revised June 29, 2015, December 16, 2015, February 29, 2016, and May 8, 2016; accepted June 3, 2016. This work was supported in part by the Natural Science Foundation of China under Grants 61572198, 61321064, 61370190, 61173154, 61472429, and 61532021; by the
Priority Academic Program Development of Jiangsu Higher Education Institu- tions; by the Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology; by the European Commission under Grants H2020-644024 and H2020-700540; by the Government of Catalonia through the ICREA Acadèmia Prize and Grant 2014 SGR 537; and by the Spanish Government under Grants TIN2014-57364-C2-1-R and TIN2015-70054-REDC. The Associate Editor for this paper was L. Yang.

L. Zhang and C. Hu are with Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, Shanghai 200062, China; with State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China; and also with Nanjing University of Information Science and Technology, Nanjing 210044, China (e-mail: leizhang@sei.ecnu.edu.cn).
Q. Wu is with School of Electronics and Information Engineering, Beihang University, Beijing 100191, China; and also with State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences; State Key Laboratory of Cryptology, Beijing 100878, China (e- mail: qianhong.wu@buaa.edu.cn).
J. Domingo-Ferrer is with the Department of Computer Engineering and Maths, Universitat Rovira i Virgili, 43003 Tarragona, Catalonia (e-mail: josep. domingo@urv.cat).
B. Qin is with Key Laboratory of Data Engineering and Knowledge Engineering, Ministry of Education, School of Information, Renmin University of China, Beijing 100872, China; with Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan 250100, China; and also with State Key Laboratory of Cryptology, Beijing 100878, China (e-mail: bo.qin@ruc.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.
Digital Object Identifier 10.1109/TITS.2016.2579162

conditions) to/from nearby vehicles and RSUs. These messages reduce the drivers' risk of having an accident and help them manage small emergencies.

It is essential to ensure that the safety-related messages are authenticated, non-repudiable and unmodified. Otherwise, a malicious vehicle could send fraudulent messages for its own profit or impersonate other vehicles to launch attacks without being caught. Vehicle privacy is also a critical concern. In VANETs, a vehicular message usually contains information on a vehicle's speed, location, direction, etc. From those messages, a lot of private information about the driver can be inferred. Furthermore, malicious vehicles may send fake messages to misguide other vehicles into accidents. This implies that privacy should be conditional in the sense that the message generators should be traceable when fake messages cause harms. For this purpose, the vehicle-generated messages must be stored by the receiving vehicles and other entities (e.g., the traffic management authority). In VANET, each vehicle broadcasts a message to nearby vehicles and RSUs every few hundreds of milliseconds. A vehicle or an RSU may receive hundreds of messages in a short period. If the messages cannot be processed in time, traffic jams and even accidents may ensue. Hence, it is critical to devise security and privacy

mechanisms that do not lead to an unaffordable reaction delay.

A. Related Work

At least five categories of proposals have addressed security and privacy concerns in VANETs. The first category is based on digital signatures combined with anonymous certificates (e.g., [6], [7]). The signatures can provide message integrity, authentication and non-repudiation. To cope with the privacy issue, digital signatures must be combined with short-lived anonymous certificates. Accordingly, each vehicle needs to pre-load a huge pool of anonymous certificates to achieve vehicle privacy; the trusted authority suffers from a heavy certificate management burden to maintain all the anonymous certificates of all the vehicles.

The second category is based on group signatures (e.g., [8]– [12]). This approach is free from traditional certificate management. However, for practical deployment, group signature based protocols need to be improved in several aspects. Their main deficiency is the member revocation problem, that is, how to exclude the revoked and compromised signers without degrading their privacy (an open question in cryptography) or the efficiency of the system. Besides, the verification and transmission/storage costs of a group signature are usually sev-eral times higher than those of a traditional signature. In [10], Zhang et al. introduced an on-the-fly group creation approach to eliminate the member revocation problem. However, their method assumes that the RSUs are fully trusted. Also, the overheads of signature verification and transmission/storage of [10] are still high.

The third category is based on identity-based cryptography (IBC) (e.g., [13], [14]). In IBC, an entity uses a recognizable identity as its public key and its private key is generated by a trusted authority (TA) using a master secret. To achieve privacy, the identity of an entity is replaced with pseudonyms. This approach is similar to the one based on anonymous certificates and hence suffers from a similar problem of heavy pseudonym management burden.

The fourth category, e.g., the IBV protocol in [15], is based on an ideal tamper-proof device (TPD) (i.e., a device from which no attacker can ever extract any stored data) using a variant of IBC. It requires the master secret of TA to be stored in a TPD. This approach can avoid certificate management and achieve unlinkable privacy (a.k.a. unlinkability and defined in Section II- B). However, the assumption of ideal TPDs is too strong to be practical. In practice, manufactured TPDs can be expected to resist known attacks, but not all future attacks. Even if an attacker cannot probe the inside of a TPD, he might collect substantial information through side-channel attacks [16].

The final category, e.g., the APPA protocol [17], is built on a one-time identity-based aggregate signature (OTIBAS) and the multiplicative secret sharing (MSS) technique [16], and, also requires the master secret (shares) of TA to be stored in a TPD. MSS is used to achieve leakage resiliency, i.e., the scheme remains secure in the presence of bounded information leakage of the master secret stored in the TPDs. Yet, a leakage-resilient scheme cannot withstand an obstinate attacker who continually places the TPD under a long-term side-channel attack. In fact, this attack strategy is attractive and practical for criminals, since, once the master secret is extracted, they can fully control the entire VANET.

B. Our Work

Existing proposals to secure VANETs suffer from time-consuming cryptographic operations, huge volume of crypto- graphic data, costly certificate/pseudonym management and/or reliance on ideal TPDs. To mitigate these issues, we present a new security tool called multiple-TA OTIBAS (MTA- OTIBAS) and based on it we propose an efficient distributed aggregate privacy-preserving authentication (DAPPA) protocol for secure vehicular communications.

An MTA-OTIBAS scheme consists of a root TA, several lower-level TAs and users. Each lower-level TA is enrolled by the root TA. A user can register to any lower-level TA and compute a signature on a message if the user has obtained a private key from the lower-level TA. The signature is only valid under the user's identity and the public information of the lower- level TA. An MTA-OTIBAS scheme has the following features. Firstly, each user's public key is his identity, which avoids certificate management. Secondly, a signer's private key, associated with an identity and a lower-level TA, is restricted to be used only once and will be updated after each use. Thirdly, the MTA-OTIBAS scheme allows numerous signatures to be aggregated into a single one for fast verification and storage saving.

Based on our MTA-OTIBAS and the MSS technique [16], we propose a DAPPA protocol run among a root TA, RSUs and ve- hicles. An RSU acts as a lower-level TA of our MTA-OTIBAS scheme and maintains the vehicles in its management area. Each RSU is assumed to be semi-trusted (see Section II-A) and has a private/public key pair valid for a period of time (e.g., one day). When a vehicle enters the management area of an RSU and is authenticated, the RSU sends the shares of its private key and the authorized period to the vehicle. The vehicle can only use the shares within the authorized period; once the shares expire, they are deleted. With the shares and the MSS technique, the vehicle can generate one-time pseudonym-private key pairs and leakage- resilient MTA-OTIBASs locally. If an authenticated message is later found to be fake, the root TA can recover the real identity of the vehicle. In this way, the security and (conditional) unlinkability requirements are met.

We note that message distribution in VANET can exploit two antipodean distributed paradigms: beaconless or beaconed. For the purpose of unlinkability, we suggest to adopt the beaconless approach. However, this is not mandatory and it is also feasible to use beacons. To this end, one can add a reusable header to several one-time pseudonyms. Then these pseudonyms can be linked to a single vehicle. This variant, like traditional pseudonym-based schemes, cannot achieve unlinkability, that is, the vehicular messages can be linked to the vehicle, although the vehicle stays as anonymous as linkage allows.

We emphasize that DAPPA has a robust system architecture and relies on a more realistic TPD. Firstly, our system addresses the key escrow problem. The root TA cannot learn a vehicle's secret shares from the RSUs while

the RSUs cannot learn the vehicle's secrets issued by TA. Hence, no other single entity can learn the full secrets of a vehicle and hence generate signatures to frame the vehicle. This is different from the existing identity- based privacy-preserving protocols, in which the TA knows all the secrets of the vehicles. Secondly, unlike [15], [17], the system master secret in DAPPA is merely known to the root TA. If a vehicle is corrupted, only a limited number of vehicles (those within the cover range of some RSUs) can be affected. Further, the secrets stored in the TPD can be updated before the attacker extracts sufficient secret information. This is important because an obstinate attacker is likely to recover the secret in a TPD after long-term trials, especially with new attack approaches and increasing computing power.

2. BACKGROUND

A. System Architecture

As shown in Fig. 1, the proposed system consists of a root trusted authority (TA), a number of RSUs and vehicles.

The root TA generates the global system parameters and mas- ter secret, and issues credentials for the RSUs and vehicles. In addition, TA is also responsible for recovering the real identities of the vehicles who signed and disseminated bogus messages.

The RSUs, distributed along the roadside, are assumed to be semi-trusted, i.e., honest but curious, and independent of the root TA. Each RSU maintains a management area. Each vehicle is equipped with a realistic TPD. When a vehicle enters the management area of an RSU, it registers to the RSU and receives secrets from the RSU. With the secrets, the vehicles can broadcast signed messages to nearby vehicles and RSUs.

B. Design Goals

In addition to the basic requirements of message authenti-cation, non-repudiation, and real-time processing, we keep in mind the following goals when devising our protocol:

- Conditional unlinkability. Unlinkability means the im- possibility of using the pseudonyms and signatures to identify messages originating from the same vehicle. This privacy guarantee is conditional, that is, if a bogus mes-sage is found, the root TA can find the real identity of the message generator.
- Ideal TPD freeness. The protocol employs realistic TPDs, instead of relying on ideal TPDs.
- Key escrow freeness. No entity can sign messages to frame a vehicle. In existing identity-based privacy-preserving protocols, the (root) TA can sign messages on behalf of any vehicle.

We also require message confidentiality in some specific applications, meaning that a message must be kept secret from those nodes that are not authorized to access it.

3. A NEW SECURITY TOOL: MTA-OTIBAS A. THE SCHEME

Our scheme is realized using bilinear maps. A map eˆ : G1 × α /3 G2 → GT is called bilinear if eˆ(g1, g2) =1 and eˆ(g1 g2) = eˆ(g1, g2)

for all α, /3 ∈ Z∗q , where G1, G2, GT are cyclic groups of prime order q, g1 is a generator of G1, and g2 is a generator of G2. An MTA-OTIBAS scheme involves a root TA, lower-level TAs and users, and consists of the following algorithms: Root.Setup, LowerLevel.Setup, Extract, Sign and Aggregate − Verify. Fig. 2 graphically depicts an MTA- OTIBAS scheme. We note that, in DAPPA, RSUs will act as the lower-level TAs and vehicles will act as the users. Further, we assume that the initial secrets are pre-stored in lower-level TAs and user devices before these leave the manufacturer. In this way, the secure channels can be generated using a secure key establishment protocol. Root.Setup is run by the root TA to generate the master se-cret K and the public system global parameters Y. Algorithm 1 describes the procedure. Once Y and K are generated, lower-level TAs can register to the root TA by invoking LowerLevel.Setup.

Algorithm 1 Root.Setup()

Input: Bit-length of q
Output:
1: Choose q, G_1, G_2, G_T, g_1, g_2, e, ψ and hash functions $H_0(\cdot)$: $\{0,1\}^* \rightarrow G_1$, $H_1(\cdot): \{0,1\}^* \rightarrow Z^*_q$, where ψ is a comput-able isomorphism from G_2 to G_1, with $\psi(g_2) = g_1$ [10]
2: Pick $K \in Z^*_q$, compute $y = g_2^K$
3: **return** K and $Y = (e, q, G_1, G_2, G_T, g_1, g_2, H_0(\cdot), H_1(\cdot), \psi)$

LowerLevel.Setup is run by a lower-level TA Ti. It generates the secret-public key pair and the corresponding certificate of Ti. Algorithm 2 describes the procedure. A registered lower-level TA Ti can then use Extract to generate private keys for the users.

Algorithm 2 LowerLevel.Setup()

Input: Y, the identity ID_{T_i} of a lower-level TA T_i
Output:
1: Pick $K_i \in Z^*_q$ as the secret key and set $y_i = g_2^{K_i}$ as the public key
2: Send (ID_{T_i}, y_i) to the root TA to obtain a certificate $cert_{T_i}$ which is signed using root TA's master secret
3: **return** K_i, y_i, $cert_{T_i}$

Extract is shown in Algorithm 3 and is used by a lower-level TA Ti to issue a private key for a user. The user then can run Sign to generate a signature on a message.

Algorithm 3 Extract()

Input: Y, T_i's secret key K_i, a user's identity ID_j (submitted by the user through a secure channel)
Output:
1: Compute $id_{j,0} = H_0(ID_j, 0)$, $id_{j,1} = H_0(ID_j, 1)$, $s_{j,i,0} = id^{K_i}_{j,0}$, $s_{j,i,1} = id^{K_i}_{j,1}$
2: **return** $s_{j,i} = (s_{j,i,0}, s_{j,i,1})$. $s_{j,i}$ which is passed to the user through a secure channel

Sign is depicted in Algorithm 4. The signature ak is only valid on mk under IDj and certTi . A restriction here is that a private key corresponding to a specific identity issued by a lower-level TA can be used only once. However, the

same iden-tity can be enrolled by different lower-level TAs. This implies that the corruption of a lower-level TA does not influence the users enrolled by other lower-level TAs. To verify ak, a verifier has to know certTi , which has to be sent together with ak . In DAPPA, we show an approach to save bandwidth. That is, certTi is broadcast by Ti and is obtained by a verifier (vehicle) when it is close to Ti.

Algorithm 4 Sign()

Input: Y, a message m_K, the user's identity ID_j and private key $s_{j,i}=(s_{j,i,0}, s_{j,i,1})$ issued by T_i, T_i's certificate $cert_{T_i}$
Output:
1: Compute $h_K = H_1(m_K, ID_j, cert_{T_i})$, $a_K = s_{i,i,0}^{a_K} s_{i,i,1}$
2: **return** a_K

Aggregate − Verify can be run by any user to aggregate n message-signature pairs into a single aggregate signature and check the validity of the resulting aggregate signature, as shown in Algorithm 5.

Algorithm 5 Aggregate-Verify()

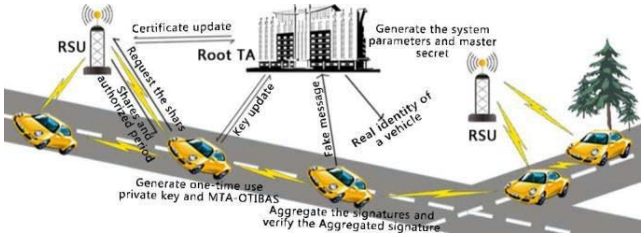
Input: Y, $\{(m_1, a_1), \ldots, (m_n, a_n)\}$ from n users enrolled by l lower-level TAs $\{T_1, \ldots, T_l\}$, identities of the users $\{ID_1, \ldots, ID_n\}$, certificates of the lower-level TAs $\{cert_{T_1}, \ldots, cert_{T_l}\}$. For simplicity, we assume $\{ID_1, \ldots, ID_{t_1}\}$, $\{ID_{t_1+1}, \ldots, ID_{t_2}\}$, $\ldots$, $\{ID_{t_{l-1}+1}, \ldots, ID_n\}$ are enrolled by $T_1, T_2, \ldots, T_l$ respectively
Output:
1: Compute $\Omega = \prod_{i=1}^{n} a_i$
2: Compute $h_j = H_1(m_j, ID_j, cert_{T_i})$ and $id_{j,0} = H_0(ID_j, 0)$, $id_{j,1} = H_0(ID_j, 1)$ for $1 \le j \le n$
3: Check $e(\Omega, g_2) = \prod_{i=1}^{l} e(\prod_{j=t_{i-1}+1}^{t_i} id_{j,0}^{h_j} id_{j,1}, y_i)$, where $t_0 = 0$, $t_1, \ldots, t_{l-1}, t_l = n$
4: **return** 1 and Ω if the equation in Step 3 holds or 0 otherwise

B. The Security of MTA-OTIBAS

The security of an MTA-OTIBAS scheme is defined by a game between a challenger CH and an adversary A. In the game, CH runs Root.Setup to obtain the system parameters, then sends the parameters to. can perform LowerLevel.Setup, Extract and Sign queries. A can also per-form a Corrupt.LowerLevel query to obtain the secret key of a lower-level TA. Finally, A outputs a forgery. We say an MTA-OTIBAS scheme is secure if no polynomial-time attacker A in the above game that does not request the private key of an entity enrolled by a uncorrupted lower-level TA can forge a valid aggregate signature for that entity.

The security of our MTA-OTIBAS scheme is based on the co-CDH assumption. That is, given (g1 , g2) for randomly chosen

a, b ∈ Z∗q , it is hard to compute g1ab. We show that if an attacker A can break our scheme, then CH can solve the co- CDH problem which is believed to be hard. For the complete proof, see the Appendix.



4. THE DAPPA PROTOCOL

A. High-Level Description

Fig. 3 graphically describes DAPPA. RSUs have a much larger communication range than vehicles. We suggest that each vehicle be equipped with a realistic TPD, in the sense that the secrets stored in the TPD must be updated before an attacker extracts sufficient information on them.

In DAPPA, the root TA generates the system parameters and master secret. Each RSU acts as a lower-level TA which has an updatable (initial) private-public key pair and a cor- responding certificate issued by the root TA. Each vehicle is pre-loaded with updatable (initial) secrets. RSUs and vehicles use their secrets to establish secure channels and/or authenticate themselves. When a vehicle enters the communication range of an RSU, it requests the shares of the RSU's private key. After authenticating the vehicle, the RSU sends the shares of the RSU's private key and an authorized period to the vehicle. The shares can only be used by the vehicle within the authorized period, and they are deleted afterwards. The vehicle uses the shares to generate its one- time use private key, and then the MTA-OTIBAS. The MTA-

OTIBASs on the corresponding messages can be aggregated and verified by other vehicles in the areas covered by the current and neighboring RSUs. If an authenticated message is found bogus, the root TA can find the originator.

B. The Protocol

Table I lists the main notations used in our DAPPA protocol.

The seven stages of the protocol follow:

System Setup: At this stage, the root TA initializes the system-wide parameters as follows:

1) Generate q, G_1, G_2, G_T, g_1, g_2, e, Ψ, pick K, $\eta \in_R Z_q^*$ as its master secret, and compute $y = g_2^K$, $e = g_1^\eta$ as its master public key. K is used to issue certificates for RSUs and η is used to establish a secure channel between the root TA and an RSU or a vehicle.
2) Choose $\mathcal{E}_\pi()/\mathcal{D}_\pi()$ and hash functions $H_0(\cdot)$: $\{0,1\}^* \to G_1$, $H_1(\cdot): \{0,1\}^* \to Z_q^*$, $H_{2key}(\cdot): \{0,1\}^* \to \{0,1\}^*$, $H_3(\cdot): \{0,1\}^* \to \Gamma$ and $H_4(\cdot): \{0,1\}^* \to \{0,1\}^*$, where $H_{2key}(\cdot)$ is a keyed hash, the key space of key is $\{0,1\}^*$, and Γ is the key space of π. Choose Λ from the key space of key.

TABLE I
NOTATION USED IN THE DAPPA PROTOCOL

Notation	Description
$\mathcal{R}_j$	The j-th RSU.
$\mathcal{V}_i$	The i-th vehicle.
$cert_{\mathcal{R}_j}$	A certificate of $\mathcal{R}_j$, issued by the root TA.
$ID_{\{\mathcal{R}_j,\mathcal{V}_i\}}$	The real identity of $\mathcal{R}_j$ or $\mathcal{V}_i$.
$IPID_{\mathcal{V}_i}$	An internal pseudo-identity of $\mathcal{V}_i$. It is generated by the root TA based on $ID_{\mathcal{V}_i}$.
$PPID_{i,t}$	The public pseudo-identity of $\mathcal{V}_i$, generated from $IPID_{\mathcal{V}_i}$ of $\mathcal{V}_i$.
$\mathcal{E}_\pi(.)/\mathcal{D}_\pi(.)$	A symmetric encryption scheme (e.g., AES), where π is the key.
$h_{\{\mathcal{R}_j,RTA\}}$	A hash-based message authentication code (H-MAC) generated by $\mathcal{R}_j$ or the root TA.

3) Keep secret (to the root TA) K, $f]$, Λ. The system parameters are $= (\hat{}e, q, G_1, G_2, G_T, g_1, g_2, y, e, \psi, H_0(\cdot), H_1(\cdot), H_{2key}(\cdot), H_3(\cdot), lE\pi(.)lD\pi(.))$. Pre-load into each vehicle and RSU.

The root TA also maintains a member list ML which is kept secret. We will define this list later.

RSU Setup: By using the LowerLevel.Setup algorithm of our MTA-OTIBAS scheme, an RSU registers as a lower-level TA. At this stage, each RSU Rj 's private-public key pair and certificate are generated. The certificate is only valid for a short period (e.g., one day). After expiration, Rj has to update its private-public key pair and the corresponding certificate.

To generate the private-public key pair, Rj picks Kj , f]j ∈ Z and the public key of Rj is (yj , ej). Kj is used to generate shares for the vehicles, and f]j is used to generate a secure channel between Rj and a vehicle. After Rj generates its public key, it submits (yj , ej) and its identifying information to the root TA through a secure channel. We can use Rj 's location information and the validity period of its public key (e.g., 1.1.2016) as Rj 's identifying information. In the end, a short-term certificate certRj is generated for Rj . certRj has the format (IDRj , (yj , ej), sigj), where sigj is a signature on (IDRj , (yj , ej)) issued by the root TA. certRj is broadcast within Rj 's communication range.

Vehicle Setup: Before Vi joins a VANET, its TPD should be initialized. Assume Vi's real identity is IDVi . When Vi joins the system, the root TA computes an internal pseudo-identity (IPID) IP IDVi = H2Λ (IDVi V Pi), and chooses an authentication key Ai, where V Pi is a validity period, e.g., "01.01.2016–01.02.2016." , IP IDVi , Ai are stored in the TPD. (IDVi , V Pi, IP IDVi , Ai) is added to ML.

Member Secrets Generation: At this stage a vehicle obtains the member secrets (shares) and an authorized period from its nearest RSU. The communications among the vehicle, the RSU and the root TA must be confidential. An RSU maintains a subgroup of a VANET. When a vehicle enters the (sub)group maintained by an RSU, if Vi already received the current mem-ber secrets from the RSU and the authorized period is not over, it does nothing; otherwise, Vi requests the member secrets and an authorized period from Rj by using the following GroupJoin protocol: 1) When Vi enters the group maintained by an RSU Rj and it does not have the current member secrets of the group, it first verifies the validity of certRj broadcast by Rj . If the signature in certRj is invalid under the master public key y, it aborts; otherwise, it extracts the identity eters are $= (\hat{}e$, q, G1, G2, GT , g1, g2, y, e, ψ, H0(·), H1(·), H2key (·), H3(·), lEπ(.)/lDπ(.)). Pre-load into each vehicle and RSU.

The root TA also maintains a member list ML which is kept secret. We will define this list later.

RSU Setup: By using the LowerLevel.Setup algorithm of our MTA-OTIBAS scheme, an RSU registers as a lower-level Vehicle Setup: Before Vi joins a VANET, its TPD should be initialized. Assume Vi's real identity is IDVi . When Vi joins the system, the root TA computes an internal pseudo- identity (IPID) IP IDVi = H2Λ (IDVi V Pi), and chooses an authentication key Ai, where V Pi is a validity period, e.g., "01.01.2016–01.02.2016." , IP IDVi , Ai are stored in the TPD. (IDVi , V Pi, IP IDVi , Ai) is added to ML.

Member Secrets Generation: At this stage a vehicle obtains the member secrets (shares) and an authorized period from its nearest RSU. The communications among the vehicle, the RSU and the root TA must be confidential. An RSU maintains a subgroup of a VANET. When a vehicle enters the (sub)group maintained by an RSU, if Vi already received the current mem-ber secrets from the RSU and the authorized period is not over, it does nothing; otherwise, Vi requests the member secrets and an authorized period from Rj by using the following GroupJoin protocol:

1) When Vi enters the group maintained by an RSU Rj and it does not have the current member secrets of the (rp, αj , /3j , Rj), and then it verifies Rj = H2πi1 (rp, αj , /3j). If the equation holds, it sets the member secrets and the authorized period in the TPD to be (αj , /3j) and rp; otherwise, it aborts. The member secrets can only be used within the authorized period. Once the period is over, the member secrets are deleted from the TPD. We note that in GroupJoin the root TA learns a vehicle's approximate region (the region of RSU Rj). A possible way to enhance the vehicle's privacy is to submit the request using a proxy. That is, (f, IDRj , j , rt) is first submitted to the proxy, and then the proxy forwards (f, j , rt) to the root TA. In practice, a vehicle can randomly choose any RSU in the system as a proxy. Hence, as long as no more than a few RSUs collude with the root TA, the latter can discover the approximate location of a vehicle only occasionally.

Vehicle Sign: A vehicular message must be signed to meet authentication, non-repudiation, and conditional unlinkability. This is achieved with our MTA-OTIBASs and the MSS technique. Suppose Vi already obtained the member secrets (αj , /3j) from its domain RSU Rj and the validity period of the member secrets is within the authorized period. Vi first generates a public pseudo-identity using IP IDVi by comput- ing P P IDi,t = H4(IP IDVi , rt), where rt is a timestamp. Then, by exploiting the MSS technique, Vi generates an MTA- OTIBAS as follows: IPID and Authentication Key Update: At this stage, Vi can update (IP IDVi , Ai). Vi can reload its IPID and authentication key using off-line and on-line modes. The first mode forces Vi to update its IPID and authentication key when it makes an official checkup (e.g., annual inspection) [20]. However, waiting for the next official checkup may leave too long a time to an attacker. Therefore, we also require Vi to periodically update its IPID and authentication key before the next official checkup, using the on-line mode. The period is configurable according to the deployment environment. The on-line model is realized using the following protocol: (rp, αj , /3j , Rj), and then it verifies Rj = H2πi1 (rp, αj , /3j). If the equation holds, it sets the member secrets and the authorized period in the TPD to be (αj , /3j) and rp; otherwise, it aborts. The member secrets can only be used within the authorized period. Once the

period is over, the member secrets are deleted from the TPD. We note that in GroupJoin the root TA learns a vehicle's approximate region (the region of RSU Rj). A possible way to enhance the vehicle's privacy is to submit the request using a proxy. That is, (f, IDRj , j , rt) is first submitted to the proxy,
and then the proxy forwards (f, j , rt) to the root TA. In practice, a vehicle can randomly choose any RSU in the system as a proxy. Hence, as long as no more than a few RSUs collude with the root TA, the latter can discover the approximate location of a vehicle only occasionally.
Vehicle Sign: A vehicular message must be signed to meet authentication, non-repudiation, and conditional unlinkability. This is achieved with our MTA-OTIBASs and the MSS technique. Suppose Vi already obtained the member secrets (αj , /3j) from its domain RSU Rj and the validity period of the member secrets is within the authorized period. Vi first generates a public pseudo-identity using IP IDVi by comput- ing P P IDi,t = H4(IP IDVi , rt), where rt is a timestamp. Then,
by exploiting the MSS technique, Vi generates an MTA-OTIBAS as follows: IPID and authentication key. This can be realized by denying Vi's request at the Member Secrets Generation stage.

C. Security and Privacy
We show that DAPPA meets the security and privacy re-quirements defined in Section II-B. Our protocol may undergo security and privacy threats in the Member Secrets Generation, Vehicle Sign and IPID and Authentication Key Update stages. Message authentication and conditional unlinkability should be met in all stages. In Member Secrets Generation, no entity ought to learn the secrets except the vehicle (more precisely, its tamper-proof device) and the RSU; and in the IPID and Authentication Key Update stage, a vehicle ought to update its IPID and authentication key confidentially. Therefore, in these two stages, we have to consider message confidentiality. Finally, the Vehicle Sign stage is mainly about secure vehicular communications: it must capture the non-repudiation property, since a vehicle may send fake messages to endanger other vehicles.
In the Member Secrets Generation stage, f is randomly generated and H3 is one-way and computationally indistinguishable, so an attacker without the knowledge of Ri or root TA's private key cannot find any information (except the length) on the one-time encryption keys πi,1 and πi,2. This is because, to compute πi,1 or πi,2, it is essential to solve the CDH problem, which is hard. Since the symmetric encryption scheme is se-cure, this stage satisfies message confidentiality. Further, IPID is used to guarantee the authentication of a vehicle. Only the root TA can learn the real identity of a vehicle. Hence, message authentication and conditional unlinkability are achieved. Since the underlying signature scheme is secure, the Vehicle Sign stage satisfies message authentication and non-repudiation. Further, the public pseudo-identities are used to blind the real identity of a vehicle and each pseudo-identity is one-time use. Since the keyed hash used to generate public pseudo-identities for the vehicle is one-way and computationally indistinguish-able, no one (except the root TA and the vehicle itself) can determine whether two different public pseudo-identities were generated by the same vehicle. This stage achieves conditional unlinkability. For the IPID and Authentication Key Update stage, similar to the Member Secrets Generation stage, Z is randomly generated, so an attacker without knowledge of the root TA's private key cannot find any information (except the length) about the one-time encryption key πi. Further, Ai is used to guarantee the authentication of a vehicle. Therefore, this stage satisfies message authentication, message confidentiality and conditional unlinkability.
Our protocol is resistant to side-channel attacks, i.e., our protocol is ideal TPD free. In DAPPA, three kinds of secrets
are stored in the TPD, i.e., IP IDVi , Ai and secret values (αj , /3j). The first one is frequently used. If Vi does not renew IP IDVi , it may leave the opportunity to an attacker to recover this secret, so that the attacker can trace Vi. In DAPPA, IP IDVi can be updated. Before an attacker collects enough side- channel information to recover the current secret IP IDVi , the latter is already updated. In the worst case, even if the attacker recovers IP IDVi , the attacker can only track the vehicle for a short period of time, i.e., before IP IDVi is renewed. The second
secret, Ai, is only used for vehicle authentication and can be updated. It is much harder for an attacker to recover this secret through side-channel attacks than to recover IP IDVi
. In fact, all

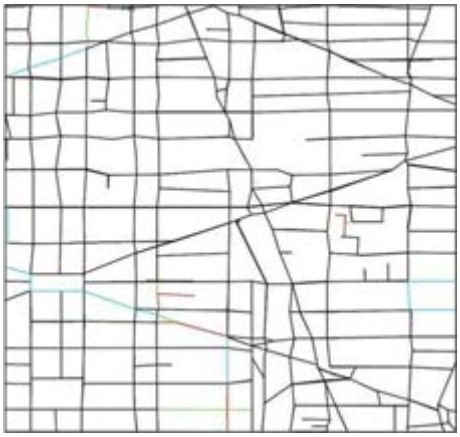


Fig. 4. Simulation scenario 2 × 2 k 2.

D. Resistance to False Messages
False messages (i.e., invalid message-signature pairs) may degrade the system performance. This may be caused by chan-nel noise and malicious vehicles. The noise infection can be eliminated with error-correcting codes. A malicious vehicle may generate seemingly correct messages to cheat other ve-hicles. This attack is more related to denial-of-service (DoS) and Sybil attacks, that cannot be fully avoided by cryptographic schemes. The DoS and Sybil attacks in wireless networks have been extensively investigated. For example, one could use the method in [18] to detect whether the received message is false or not. Further, the localization technique [19] can be applied to estimate the location of the originator of a malicious message.

5. SIMULATIONS

We performed simulations using NS-2 to evaluate the perfor-mance of our protocol. The simulations were run on a Linux machine using an Intel Core i7-3770 at a frequency of 3.4 GHz. We implemented an MNT curve of embedded degree k = 6 and 160-bit q. The simulated area is shown in the

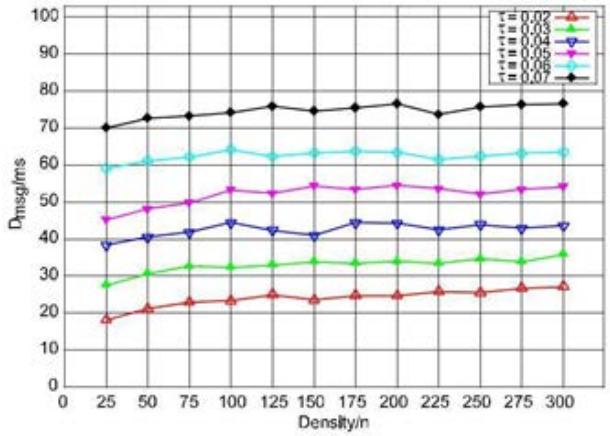


Fig. 5. Message authentication delay in the ideal case.

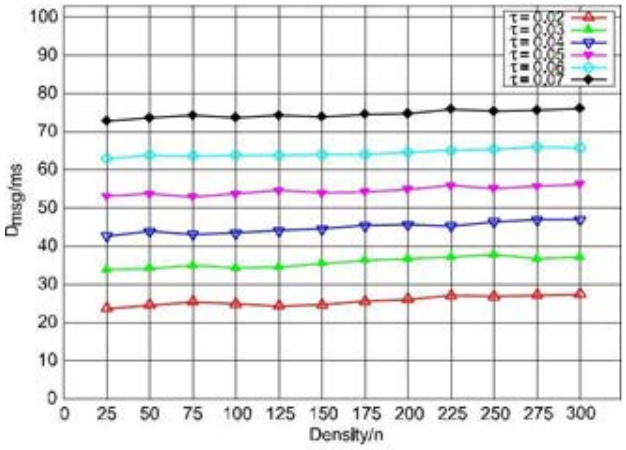


Fig. 6. Message authentication delay on average.

M AD is the maximum allowable delay, i.e., 100 ms [2]. Dmsg must be smaller than M AD. D is the sample district, the total number of vehicles in D is LD, the total number of messages sent by a vehicle is M → , K is the number of vehicles within m a one-hop range of vehicle , Tsgn→ is the time cost for to sign The simulation results are shown in Figs. 5–7, which reflect the relationship among Dmsg, the vehicle density and the batch verification period r . It is easy to see that in all conditions, the delay is less than M AD. Fig. 5 shows the message authentication delay in the ideal case, in which a vehicle can only receive messages from its own group. Fig. 6 shows the message authentication delay on average, in case a vehicle can receive messages from one to four groups. Fig. 7 shows the message authentication delay in the worst case, in which a vehicle receives messages from four groups. In all the simulation results, Dmsg increases with r for fixed vehicle density. For a fixed r ,

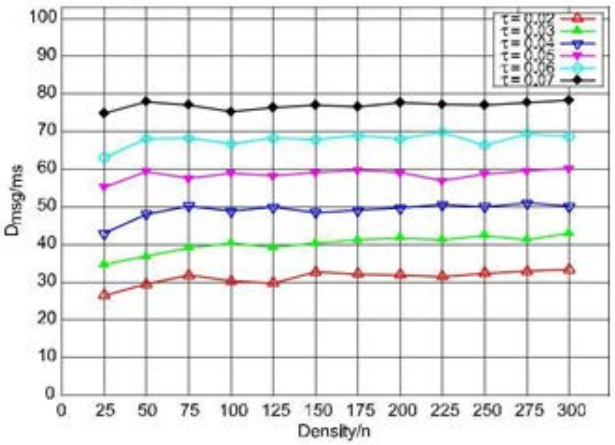


Fig. 7. Message authentication delay in the worst case.

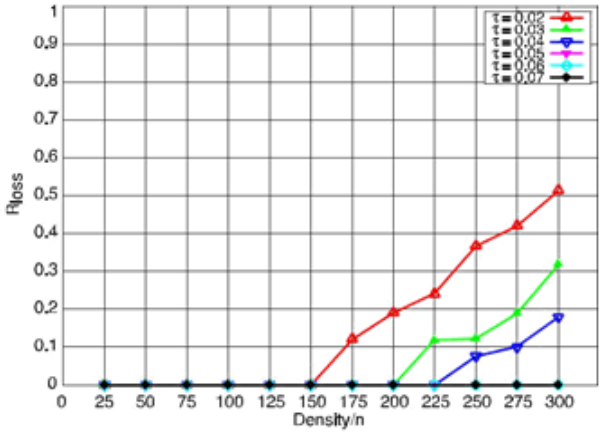


Fig. 8. Message-loss rate in the ideal case.

the delay is mainly determined by the batch verification period, and grows only a little as the vehicle density grows. This is due to the fact that most received messages can be verified on time.

If messages received by a vehicle cannot be processed in a batch verification period, some messages will be dropped, which results in message loss. The average message loss rate is defined as where nr is the maximum number of messages that a vehicle

can verify in r , and nvi is the number of messages that vi received in a given r .

Figs. 8–10 show the message loss rate in the ideal case, on average and in the worst case, respectively. In all figures, it is easy to see that, when r ≤ 40 ms and the density of vehicles is high, there is a high message loss rate. This is because the batch period is too short, so that only a few messages are received, and the advantage of batch verification is not well exploited. When

τ ≥ 50 ms, the message loss rate tends to 0. Considering the message authentication delay in the above simulation and the requirement that the delay should be as small as possible, we have the result that r = 50 ms seems an ideal balance point.

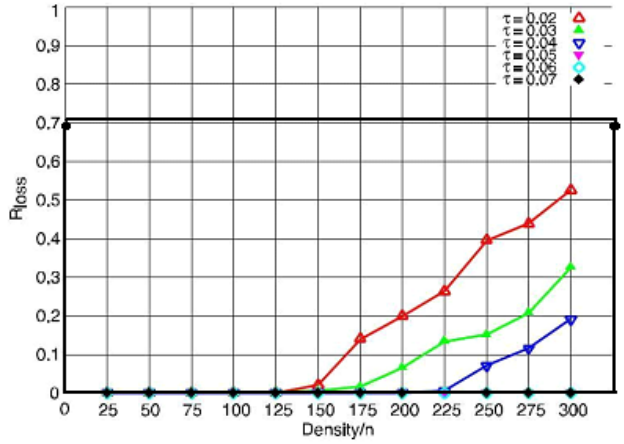


Fig. 9. Message-loss rate on average.

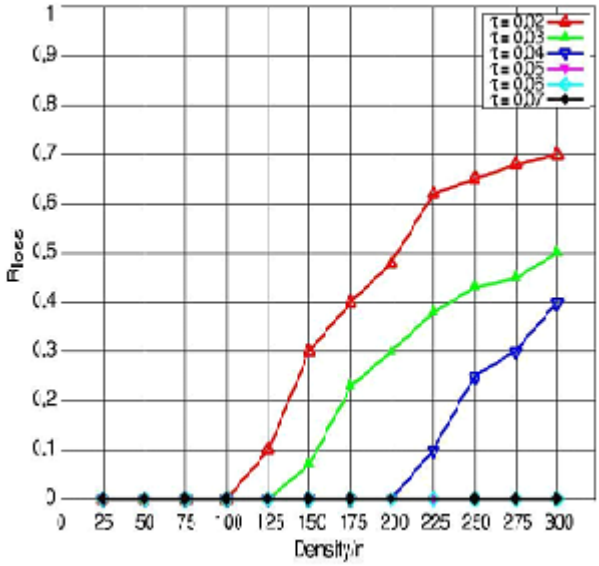


Fig. 10. Message-loss rate in the worst case.

We also compare the verification cost our protocol with those of IBV in [15] and APPA in [17], which are in the same family, and also with the standard ECDSA-based protocol in [1] and a recent identity-based aggregation (IBA) scheme [14]. We will not compare the verification cost of our protocol with those based on group signatures, since even the most efficient group signature scheme is several times less efficient than the underlying signature scheme in our protocol and the advantage of our protocol is obvious. We note that the original IBV and APPA assume that all the vehicles are enrolled by a single TA. For better comparability, we extend IBV and APPA to a multiple TA environment.

Fig. 11 shows that our protocol is more efficient than the ECDSA-based one in all cases, and more efficient than IBA on average and in ideal case. In the worst case, our protocol is more efficient than IBV and APPA, and has comparable efficiency to IBA. However, unlike IBA, our protocol avoids the heavy pseudonym management problem. On average, our protocol is about 1.5 times more efficient than APPA, and has comparable efficiency to IBV. In the ideal case, our protocol is as efficient as APPA, and slightly less efficient than IBV. However, unlike our MTA-OTIBAS scheme, IBV and APPA rely on the existence of ideally TPDs.

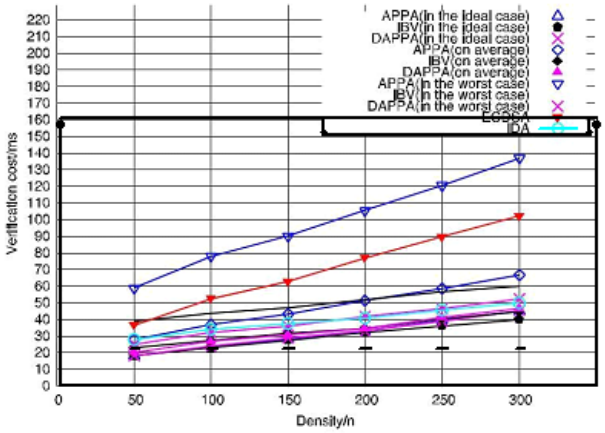


Fig. 11. Comparison.

A. Vehicle Authentication Efficiency

In our protocol, when a vehicle requests its member secrets from its nearby RSU at the MemberSecretsGeneration stage, the vehicle must be authenticated by the RSU with the help of the root TA. If a VANET contains a huge number of vehicles, then it will be a challenge for the root TA to authenticate the vehicles for the RSUs. For example, consider a VANET with 1 million vehicles and assume 10% of the total vehicles are driving. Assume further a vehicle has to request its member secrets from an RSU about every 2 minutes on average. Hence, the root TA will receive 50,000 requests in one minute on av-erage. For a single request, each vehicle needs to send 57 bytes of encrypted data to the TA and the root TA just needs about 0.3 ms to authenticate the vehicle. Hence, in total, the root TA needs about 150 s to authenticate all the requests. In order to an-swer those request in real time, the root TA needs at least three authentication servers. Further, the bandwidth requirement is about 0.36 Mbps. If a million of vehicles were on the road, the bandwidth requirement would be about 3.6 Mbps.

B. Tracing Efficiency

To find the real identity of a message sender with cor-responding PPID P P ID?,?, the root TA searches ML for a tuple (IDVi , V Pi, IP IDVi , Ai) such that H4(IP IDVi , rt) = P
P IDV?,? . If the equation holds, the root TA outputs IDVi . If SHA-1 is chosen, it only takes 0.0005 ms on average for the root TA to perform a hash operation. If there are 1 million
vehicles in the system, it takes less than one second to find the real identity of the message sender.

6. CONCLUSION AND FUTURE WORK

We proposed the DAPPA protocol for secure vehicular communications. DAPPA achieves enhanced privacy (i.e., condi-tional unlinkability), key escrow freeness, robustness and fast message processing, without requiring an ideal TPD. Simula-tions show that our protocol is practical.

As future work, it would be interesting to address the mes-sage broadcast problem in extreme cases (e.g., when a traffic IEEE Trial-Use Standard for Wireless Access in

Vehicular Environments-Security Services for Applications and Management Messages,

REFERENCES

[1] IEEE Std.1609.2-2013. [Online]. Available: https://standards.ieee.org/findstds/ standard/1609.2-2013.html

[2] "Legislative resolution on the proposal for a directive of the European parliament and of the council on the retention of data processed in connection with the provision of public electronic communication services and amending directive 2002/58/EC," Eur. Parliament, Brussels, Belgium, (COM(2005)0438 C6-0293/2005 2005/0182(COD)), 2005.

[3] V. Daza, J. Domingo-Ferrer, F. Sebé, and A. Viejo, "Trustworthy privacypreserving car-generated announcements in vehicular ad hoc networks," IEEE Trans. Veh. Technol., vol. 58, no. 4, pp. 1876–1886, May 2009.

[4] F. Qu, Z. Wu, F. Wang, and W. Cho, "A security and privacy review of VANETs," IEEE Trans. Intell. Transp. Syst., vol. 16, no. 6, pp. 2958– 2996, Dec. 2015.

[5] X. Wen, L. Shao, Y. Xue, and W. Fang, "A rapid learning algorithm for vehicle classification," Inf. Sci., vol. 295, no. 2015, pp. 395–406, 2015.

[6] M. Raya and J. Hubaux, "The security of vehicular ad hoc networks," in Proc. SASN, 2005, pp. 11–21.

[7] M. Raya and J. Hubaux, "Securing vehicular ad hoc networks," J. Comput. Security, vol. 15, no. 1, pp. 39–68, 2007.

[8] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacypreserving protocol for vehicular communications," IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3442–3456, 2007.

[9] Q. Wu, J. Domingo-Ferrer, and U. González-Nicolás, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," IEEE Trans. Veh. Technol., vol. 59, no. 2, pp. 559–573, Feb. 2010.

[10] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," IEEE Trans. Veh. Technol., vol. 59, no. 4, pp. 1606–1617, May 2010.

[11] X. Zhu, S. Jiang, L. Wang, and H. Li, "Efficient privacy-preserving authentication for vehicular ad hoc networks," IEEE Trans. Veh. Technol., vol. 63, no. 2, pp. 907–919, Feb. 2014.

[12] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, and B. Liu, "Practical secure and privacy-preserving scheme for value-added applications in VANETs," Comput. Commun., vol. 71, no. 2015, pp. 50–60, Nov. 2015.

[13] J. Li, H. Lu, and M. Guizani, "ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 4, pp. 938– 948, Apr. 2015.

[14] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, "Privacypreserving vehicular communication authentication with hierarchical aggregation and fast response," IEEE Trans. Comput., to be published, doi: 10.1109/TC.2015.2485225.

[15] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identitybased batch verification scheme for vehicular sensor networks," in Proc. IEEE INFOCOM, 2008, pp. 246–250.

[16] E. Kiltz and K. Pietrzak, "Leakage resilient ElGamal encryption," in Proc. ASIACRYPT, 2010, pp. 595–612.

[17] L. Zhang, Q. Wu, B. Qin, and J. Domingo-Ferrer, "APPA: Aggregate privacy-preserving authentication in vehicular ad hoc networks," inProc. ISC, 2011, pp. 293–308.

[18] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in Proc. VANET, 2004, pp. 29–37.

[19] C. Laurendeau and M. Barbeau, "Probabilistic localization and tracking of malicious insiders using hyperbolic position bounding in vehicular networks," EURASIP J. Wireless Commun. Netw., vol. 2, pp. 1–13, 2009.

[20] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in Proc. HotNets-IV, 2005, pp. 1–6.