Hindawi
Mobile Information Systems
Volume 2017, Article ID 4682538, 11 pages
https://doi.org/10.1155/2017/4682538

Research Article

Obfuscated RSUs Vector Based Signature Scheme for Detecting Conspiracy Sybil Attack in VANETs

Xia Feng[1,2] and Jin Tang[2]

[1]*Department of Computer Science & Technology, Anhui University, Hefei, Anhui 230601, China*
[2]*School of Computing, The University of Utah, Salt Lake City, UT 84102, USA*

Correspondence should be addressed to Xia Feng; fengx.ahu@foxmail.com

Received 11 August 2016; Revised 11 December 2016; Accepted 22 December 2016; Published 7 February 2017

Academic Editor: Stefania Sardellitti

Given the popularity of vehicular Ad hoc networks (VANETs) in traffic management, a new challenging issue comes into traffic safety, that is, security of the networks, especially when the adversary breaks defence. Sybil attack, for example, is a potential security threat through forging several identities to carry out attacks in VANETs. At this point, the paper proposed a solution named DMON that is a Sybil attack detection method with obfuscated neighbor relationship of Road Side Units (RSUs). DMON presents a ring signature based identification scheme and replaces vehicles' identities with their trajectory for the purpose of anonymity. Furthermore, the neighbor relationship of RSUs is obfuscated to achieve privacy preserving of locations. The proposed scheme has been formally proved in the views of security and performance. Simulation has also been implemented to validate the scheme, in which the findings reveal the lower computational overhead and higher detection rate comparing with other related solutions.

1. Introduction

Generally, VANETs require that all connected vehicles register with given identity codes, just as the Plata Number in reality [1]. However, most vehicle users expect their identity information can be preserved in VANETs for they are afraid that their traveling will leak with the identity. Thus, anonymous methods are employed to hide their privacy [1, 2]. Sybil attack is a typical security thread from malicious vehicles, which can take more communication resources or offline economical profits through multiple identities [3]. The false traffic messages from attackers not only cause congestions but also increase risk of traffic accidents [1, 4].

Most recent Sybil detection methods can be grouped in two types: hardware based scheme [5–8] and cryptology based identification method [9–13]. The hardware based scheme commonly applies technologies of signal strength [5–7] or resource testing [8]. However, the overdependence on hardware restrains its application; moreover, high cost in hardware improvements is another drawback for users to connect their vehicles to VANETs. The cryptology based scheme adopts identity authentication technology which is independent of vehicles and compatible with identity based management system [1]. Thus, the cryptology based scheme becomes the main solution for attack detection in VANETs. Although network users benefit from identity authentication and attack detection technologies, risks still exist in preserving users' privacy.

Conspired Sybil attacks are first presented in [14], in which attackers can masquerade as conspiracy vehicles using their identities in order to send malicious messages to other vehicles nearby. However, the conspired Sybil attacks cannot be prevented efficiently due to the weakness of current detection scheme supposing identities are always held securely. According to Sybil attack detection, reputation system based scheme was presented in [14]. Reputation system issues a trust value for each node, which can be reduced by an distrustful or malicious behaviour [15–17]. Thus, Sybil attackers can be distinguished based on the trust value. The identities with lower values will be considered as malicious nodes and

ruled out no matter where these identities come from, either bound vehicles or faked attackers. However, as noted in [17], two significant features should be considered for VANETs: firstly, VANETs do not allow decreasing the reputation after the serious traffic accidents to prevent another attack, because the damage of life and things in this attack cannot be repaired; secondly, most vehicles replace their identities with pseudonyms or authorized messages to achieve privacy preserving, and it is difficult to associate an ID to a vehicle and a trust value to an ID, respectively.

This paper proposes a method that completes identity certificate through tracing vehicles' wheel path based on RSUs. The method authenticates vehicles' identification in an anonymous manner just as the trajectory based signature scheme in Footprint [10, 18]. RSUs' neighbor relationship is also obfuscated to prevent trajectory privacy from being leaked to RSUs and other vehicles. Our main contributions can be highlighted as follows:

(i) A ring signature scheme is proposed as secret material to generate identity certificate of vehicles. The signature includes a vector with concealment information of the signing RSU's neighbor relationship.

(ii) Location privacy is preserved by obfuscating the mapping function between relationship vector and RSUs' adjacent connections. However, the obfuscated vector still marks and conceals the RSU's neighbors.

(iii) A method is presented to compute the adjacent connection of two RSUs using the obfuscated vectors of two RSUs. In the methods, RSUs and vehicles can obtain the result whether two RSUs are located in two-hop neighbor area without knowing the relationship concealed in vector.

The rest of the paper is organized as follows. Section 2 describes the related work and an example of conspiracy Sybil attack. Section 3 illustrates the architecture of VANETs and the research objectives. Section 4 gives a brief description of the protocol. Section 5 conducts performance evaluation of the proposed method. Section 6 concludes the whole research.

2. Related Work

Sybil attack is an attack by forging multiple identities which is firstly presented in peer-to-peer networks by Douceur [19]. Factually, Sybil attack also happens in ad hoc networks [3], sensor networks [7, 20], and VANETs [6, 9, 10]. This work will focus on an identity authentication scheme that benefits from the identification based Sybil attack detection.

Pseudonyms are firstly used as a privacy protected scheme for identification of vehicles. Zhou et al. [9] proposed a pseudonym based Sybil attack detection scheme for privacy preserving. In the scheme, the Trust Authority distributes a number of pseudonyms for each vehicle. Abused pseudonyms can be detected by RSUs. Since RSUs are heavily involved in the detection process, this scheme requires the full coverage of RSUs in the field and makes RSUs a little overloading in computation and communication. What is worse, in such a scheme, vehicles should be managed by a centralized trusted center. If there is no an online centralized trusted center, pseudonyms based identification is invalid to conspiracy Sybil attack, for the attacker can borrow some pseudonyms from the conspired vehicles, and it is difficult to detect because each vehicle has many pseudonyms. Each time RSU detects suspicious pseudonyms, it should send all the pseudonyms to the trust center for further decision, which makes the trust center be the bottleneck of the detection.

Lee et al. [11] lighten RSUs' load by only relaying message for vehicles, and malicious vehicles will be recognized by a local VANET server (LCertVANET). Hussain et al. [12] proposed a privacy-friendly RSU driven Sybil attack detection, in which vehicle should have obtained "tokens" from BRSU before reporting any event. Lin et al. [13] proposed an efficient local Sybil resistance scheme. In [13], RSU periodically broadcasts an authorized time stamp to vehicles in its vicinity as the proof of appearance at this location. Vehicles collect these authorized time stamps which can be used for future identity verification. Park et al. [21] present an approach where RSUs are the only components issuing the certificates. In these schemes, if a vehicle signs two or more signatures at the same time period, it would be judged as the Sybil vehicle. In these methods, a different method for identification was presented, in which vehicles obtain secret materials from authorized Trust Authority (TA) to generate their tokens served as the identity certificates, but vehicles' unique ID and master key are registered and downloaded from a VANET server and will not be revealed in the authentication process. Unfortunately, the failure of any RSU will lead to no relaying message, no tokens, and no stamps; then vehicles near the failed RSU will be unable to report any event in the scheme.

The Sybil detection schemes in [10, 18] utilize location information to realize identification. Footprint [10] has been proposed to use the trajectories of vehicle for identification while still preserves the anonymity and location privacy of vehicles. However, it fails in detecting conspiracy Sybil attack; in particular, the conspired identity certificates are obtained from malicious vehicles that are far away from the area of Sybil attacker.

Figure 1 shows an example of conspiracy Sybil attack: the attacker V_A came from RSU_1 to RSU_6; he will have the certificate assigned by $\{R_1, R_3, R_5, R_6\}$. If V_A has conspired with V_1, V_2, and V_3 and gets their ID materials, then he can obtain the certificate of V_1 with trajectory $\{R_2, R_3, R_5, R_6\}$ and V_2 and V_3 with trajectory $\{R_4, R_5, R_6\}$, although V_1, V_2, and V_3 did not come to RSU_6. That is to say, V_A gets 4 identity certificates and fakes that all 4 vehicles came into RSU_6; then V_A can cheat the traffic system to get more resource with his multiple identity certificate.

We proposed DMON (a Sybil attack detection method with obfuscated neighbor relationship of RSUs) in this paper, which is based on the idea of using Footprint as vehicles' identity certificates. However, the neighbor relationship of signed RSUs is set in the certificates, and the adjacent connections are obfuscated in their relationship vectors. Based on these technologies, the conspired identity certificates can be detected with the signed relationship vectors; meanwhile,

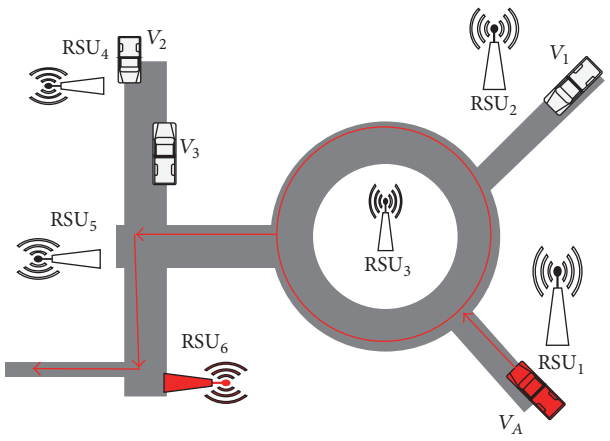


Figure 1: Example of conspiracy Sybil attack.

vehicles' locations are preserved as well as the adjacent connections of RSUs.

3. System Model and Design Objective

In vehicular networks, a moving vehicle can communicate with other neighbor vehicles or RSUs via vehicle-to-vehicle communications and roadside-to-vehicle communications. RSUs are commonly connected together and have an access to the Internet. Thus, RSUs are called road side infrastructures and the VANETs are named the Internet of Vehicles. This section will introduce key components of VANETs as well as their formal definitions and then illustrate what is conspiracy Sybil attack in detail including some security assumptions and design objectives.

3.1. System Model and Formulized Symbol. The components of VANETs in security research include Trust Authority (TA), Road Side Units (RSU), and vehicles with on-board unit (OBU), and there are two communication models: V2V (Vehicle-to-Vehicle) and R2V (RSU-to-Vehicle) communications. Figure 2 illustrates the system architecture. We illustrate the components of Figure 2 in detail as follows.

Trust Authority (TA). Trust Authority (TA) is assumed to be completely trustable and secure. In security system, TA is responsible for security operation requiring a trusted third party of the system, such as key management and secret material generation.

Road Side Units (RSU). Road Side Units (RSU) can be deployed at intersection or any area of interest to provide wireless access to vehicles as a wireless AP. All RSUs are connected with each other, have an access to Internet, and have a secure channel with TA. RSU is equipped with a wireless model and can send messages to the vehicles located in the nearby area. In this paper, we assume that there are m RSUs in the VANET, denoted as

$$\text{RSU} = \{R_1, R_2, \ldots, R_m\}. \quad (1)$$

That is to say, each RSU in VANET will map a number i, $1 \le i \le m$, and $R_i \in$ RSU is satisfied.

On-Board Unit (OBU). Vehicles are equipped with OBU. With current technologies, OBUs are capable of carrying out cryptographic computations. Vehicles call for authorized information from RSUs with OBUs. We denote that the number of vehicles in the VAET is n, and the set of vehicles could be formulized as follows:

$$V = \{V_i \mid 1 \le i \le n\}. \quad (2)$$

We also give the formulized symbol and its description in Notations; these will be used in the remainder of this paper.

3.2. Conspiracy Sybil Attack. The conspiracy Sybil attacker is based on abusing multiple identities. There are two ways to obtain the lavished identities from accomplice vehicles.

(i) Attacker takes the accomplice vehicles' identity directly as themselves.

(ii) Attacker sends the accomplice vehicles' identity to the RSU for update and then obtains a new temporal identities certificate.

If an attacker succeeds in getting identity certificate and passes the authentication, it can launch Sybil attacks. So the Sybil attack detection should be emphasized in identification. However, the conspiracy Sybil attack is different from the others for its Sybil identities are not faked but borrowed from the lavished accomplice vehicles. We conclude 3 challenges as follows.

First, the Sybil identity certificate is borrowed from the network inside vehicles, it is real and legitimate, and it has the right to pass the identification. We should recognize whether the ID certificate is used by the correct vehicle. It is more difficult than recognizing whether it is a correct certificate.

The second challenge is in the trajectory based identification. The attacker can obtain many authenticated routing messages; then he can fake a new certificate to masquerade a new trajectory based identity as illustrated in Figure 1.

Finally, the Sybil attacker can update the borrowed conspiracy identity certificate, because the attacker and the certificate are real. If the conspiracy certificate is updated by a RSU, then it is totally the same as a certificate of the attacker. Thus, conspiracy Sybil attacker should be detected before the attacker updates the conspired certificate.

3.3. Security Assumption and Design Objective. In this work, we make assumptions as in [10, 12, 21–23].

Assumption 1. Discrete logarithm problem for finite field is hard-solved.

Assumption 2. TA and all RSUs are fully trustworthy.

Assumption 3. RSUs are synchronized.

According to Assumptions 1 and 2, they are basic assumptions in security research. Assumption 3 is a little strong

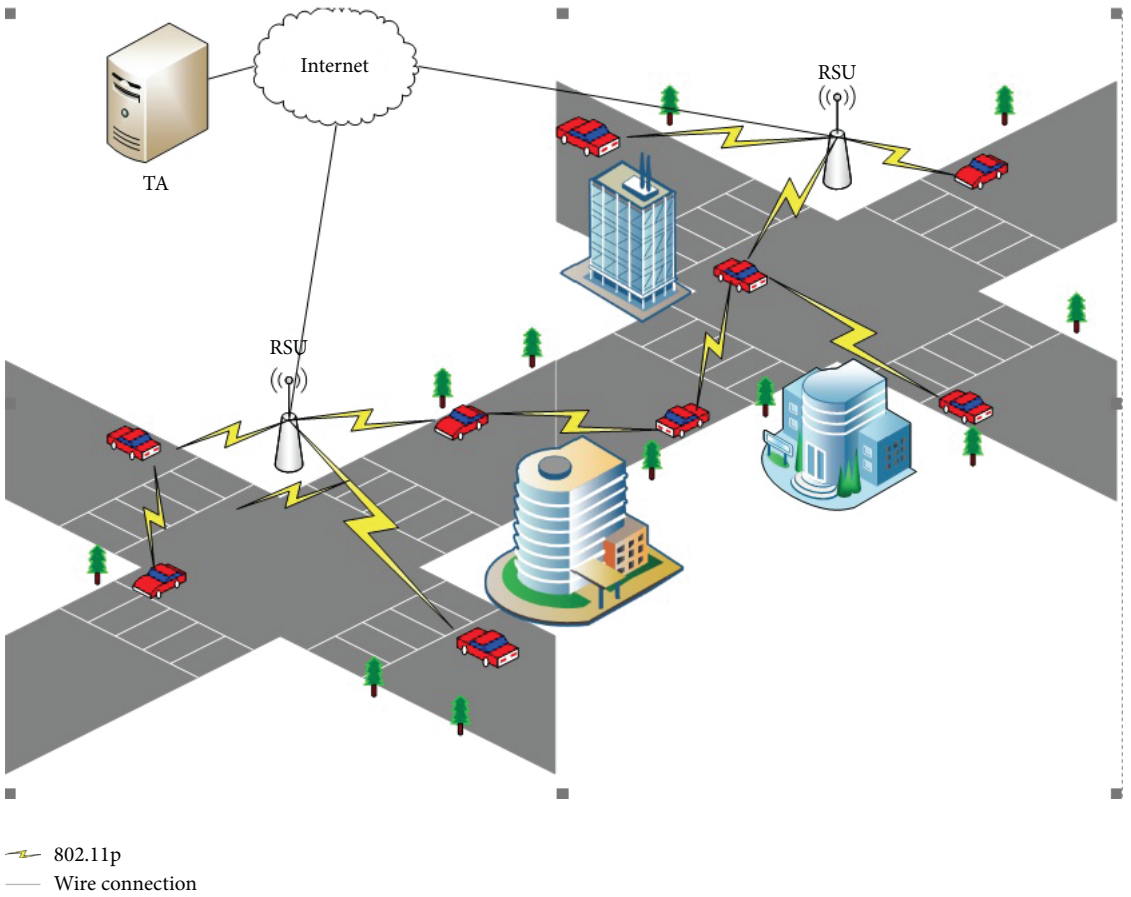


Figure 2: Architecture of VANETs.

for the practical system. But a weak synchronization among RSUs is easy to achieve since all RSUs are interconnected by the RSU backbone network in a wire manner.

In this paper, our objective is to design an identification scheme for detecting conspiracy Sybil attacker in vehicular ad hoc networks. In the meantime, the detection scheme should satisfy the following 3 items.

Privacy Preserving in Vehicles' ID and Location. Vehicles will not conceal the real unique ID Number when they apply certificate from RSUs, and the signature should be unconditional anonymity as RSUs' information is bound with the location information of passing vehicles.

Online and Independent Detection. Sybil attack should be detected and prevented before the attack starts. An offline detection may cause unbearable loss of life and property before the attack is found. The detection should also be independent, for the collaboration with other RSU will conduct more information leakage and require higher density of RSU deployment.

High Efficiency and Low Overhead. Due to the high mobility of vehicles, signature and authentication program should also consider the efficiency requirements in terms of low computation overhead and rapid authentication.

4. DMON

DMON is a Sybil attack detection method using obfuscated neighbor relationship of RSUs, which is based on cryptographic ring signature. We set a label vector of the signing RSU's neighbor relationship into a ring signature scheme [22] to obtain unconditional anonymity and linkable attribution and then hide the adjacent connection relationship of RSU by obfuscating the label vector. Finally, we can detect the Sybil identity certificate by the relation information hidden in the label vectors.

4.1. System Initialization

Initializing TA. Let G be a group of prime order p such that the underlying discrete logarithm problem is intractable. Let $H : \{0,1\}^* \to \mathbb{G}$ and $H' : \{0,1\}^* \to \mathbb{Z}_p$ be two hash functions. The TA chooses two public parameters $g \in \mathbb{G}$, $h \in \mathbb{G}$. The TA generates the public parameters Sys_P as follows:

$$\text{Sys\_}P = \left\{\mathbb{G}, \mathbb{Z}_p, H, H', g, h, \text{PKL}, \Delta t\right\}, \tag{3}$$

where PKL is the list of RSUs' public key and Δt is the life period of a RSU signature. The Sys_P will be downloaded into the registered RSU and vehicles.

Setting Up RSUs. Each RSU, denoted as R_i, joins the VANET; TA will send R_i a pair of keys of public cryptology system

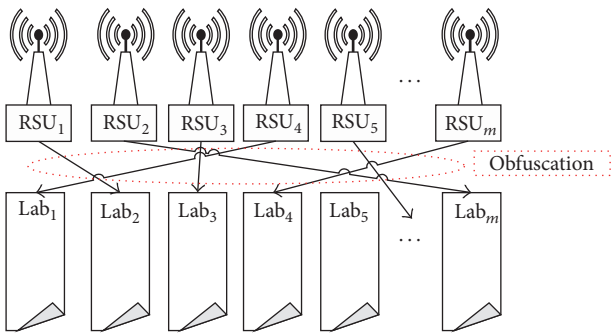


Figure 3: Obfuscated mapping from RSU to label vector.

(Key_pub$_i$, Key_sec$_i$) and save the public key of this key pair in its Public Key List (PKL) of the public parameters Sys_P. More specifically, when a new RSU enrolls in the system, TA will update the PKL with a new version number and broadcast this updated PKL to all the RSUs in the system.

Setting Up Vehicles. Once a vehicle V_i gets in a VANET, it will obtain its registering information and download system parameter Sys_P from TA in an offline way, which means the vehicles should not be allowed to register in Internet. That is to say, the vehicle should be driven to a TA office and the registering information will be written in the hardware of its OBU, just as a vehicle registers in DMV (Department of Motor Vehicles) to get new plate number. Vehicles communicate with RSUs for the authorized message with a session key. TA will generate some pairs of keys for the registering vehicle, we denote the key pairs as the set $\{(V_i\text{\_pub}_j, V_i\text{\_sec}_j) \mid j = 1, 2, \ldots, k\}$, and then the vehicle can arbitrarily select a pair of key from this set to communicate with a RUS.

4.2. Obfuscation for the Relationship Vectors of RSU. After the VANET is initialized, we set a neighbor relationship matrix of RSUs, and the matrix is defined as A_RSU in (4), where the set of the neighbor nodes of R_i are denoted as neighb(R_i),

$$A\text{\_RSU}_{ij} = \begin{cases} 2 & i = j \\ 1 & R_j \in \text{neighb}\left(R_i\right) \\ 0 & \text{others.} \end{cases} \tag{4}$$

Let Lab$_j$ be a label vector of R_i ($R_i \in \{R_1, R_2, \ldots, R_m\}$), as shown in Figure 3, which is a random bijection between the column vectors of A_RSU and $\{\text{Lab}_j \mid j = 1, 2, \ldots, m\}$. Thus, the random bijection obfuscates the mapping relation between the column vectors of A_RSU and $\{\text{Lab}_j \mid j = 1, 2, \ldots, m\}$. We only know that Lab$_j$ is column vectors of A_RSU, but we do not know what is column of A_RSU; that is to say, the obfuscation hides the correlation between the vectors and RSU.

Then (5) formulized the obfuscated label matrix composed of the label vector:

$$L_{ij} = A\text{\_RSU}_{pq} \quad \text{iff } \left(\text{Lab}_i \longrightarrow R_p,\ \text{Lab}_j \longrightarrow R_q\right), \tag{5}$$

where $\rightarrow$ denotes that the label is a mapped neighbor relationship vector of the RSU and the vector of RSU is defined by (4). Usually, the ith column of L_{ij} is denoted as vector L_i. Obviously, L_i hides the neighbor relationship of a RSU (denoted as R_p), and R_p saves L_i but it does not know the hidden relationship in L_i for the mapping function from RSU to label is random and obfuscated. Further, this obfuscated mapping will be updated by TA after a certain period of time.

Lemma 4. *Let Lab$_i \rightarrow R_p$ and Lab$_j \rightarrow R_q$; if R_p is a neighbor node of R_q, then it satisfies*

$$L_i^{\,T} \cdot L_j \geq 2 \quad (i \neq j). \tag{6}$$

Proof. From (4) and (5), when R_p is a neighbor RSU of R_q, we have $L_{ij} = L_{ji} = 1$ and $L_{ii} = L_{jj} = 2$; then

$$\begin{aligned} L_i^{\,T} \cdot L_j &= \sum_{1 \leq k \leq m} \left(L_{ik} \times L_{jk}\right) \\ &\geq L_{ii} \times L_{ji} + L_{ij} \times L_{jj} = 2 + 2 = 4 > 2. \end{aligned} \tag{7}$$

Thus, (6) is satisfied. In Lemma 4, we assume that a node is not the neighbor of itself, so we let $i \neq j$. In fact, if we define that $A\text{\_RSU}_{ij} = 1$ when $i = j$ in (4); then the following equation is obtained:

$$L_{ii} \times L_{ji} + L_{ij} \times L_{jj} = 2. \tag{8}$$

Equation (6) is still satisfied.

For clearance in illustration, we denote the label vector of R_p as $L(R_p)$, when Lab$_i \rightarrow R_p$; that is,

$$L\left(R_p\right) \equiv L_i \quad \text{when Lab}_i \longrightarrow R_p. \tag{9}$$

□

4.3. Ring Signature Based Identification. In DMON, registered vehicles should apply signed messages from the RSU they are passing, and the signature will be used as the secret materials to generate their identity certificates. And an identity certificate will be updated if the owned vehicle passes the authentication of another RSU. The signature of RSU, the identity generation, and the updating process will be discussed in this subsection.

4.3.1. Temporal Identity Generation. When a vehicle V_i approaches a RSU, denoted as R_p, it calls for authorized messages by sending one of its public keys $M_0 = V_i\text{-pub}_j$ to R_p. Then R_p generates a message M_1 as follows:

$$M_1 = \left(t_s, V_i\text{-pub}, L\left(R_p\right)\right), \tag{10}$$

where $L(R_p)$ is the obfuscated label vector as defined by (9) and t_s is the sending time recorded from V_i's application message that belong to period $[t_k, t_{k+1}]$ as mentioned before.

Then R_p signs the message M_1 and obtains Sign_$R_p(M_1)$. Considering the location privacy, we chose Liu et al. [22] ring signature scheme to provide the RSU anonymity for its security and efficiency.

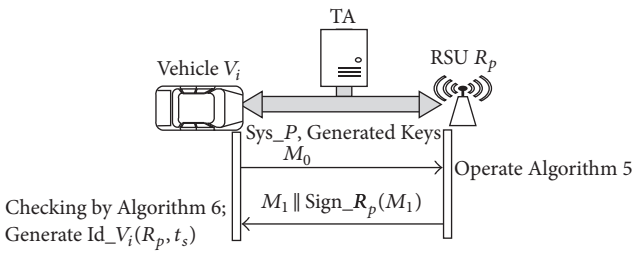


Figure 4: Temporal identity generation protocol.

After receiving M_1, vehicle V_i encrypts $\text{Sign\_}R_p(M_1)$ by the secret key of the pair $(V_i\text{-pub}_j, V_i\text{-sec}_j)$ and obtains the core material of its temporal identity $\text{Id\_}V_i(R_p, t_s)$; that is,

$$\text{Encrypt\_}V_i\text{-sec}\left(\text{Sign\_}R_p\left(M_1\right)\right) \propto \text{Id\_}V_i\left(R_p, t_s\right), \tag{11}$$

where symbol $\propto$ illustrates that $\text{Encrypt\_}V_i\text{-sec}(\text{Sign\_}R_p(M_1))$ is only a core component and is not equal to $\text{Id\_}V_i(R_p, t_s)$. The complete description of $\text{Id\_}V_i(R_p, t_s)$ is given in (16).

Figure 4 gives a concise illustration for the temporal identity generation protocol, and the detailed description of the algorithms in the protocol is as follows. It is assumed that the system is driven by the time period event. We denote that the current time t_s belongs to time period $[t_k, t_{k+1}]$, and the public key pair of R_p is $(\text{Key\_pub}_p, \text{Key\_sec}_p)$. In discrete logarithm based signature, we denote that

$$\text{Key\_sec}_p = (x, y), \tag{12}$$

where x and y are prime number. With the system parameters defined in (1), R_p will sign the application from V_i at the kth time period. Algorithm 5 describes the operating process of R_p in $\text{Sign\_}R_p(M_1)$.

Algorithm 5 ($\text{Sign\_}R_p(M_1)$).

Step 1. Compute $e = H(t_k)$, $\text{tag\_}R_p = e^x$.

Step 2. Randomly generate $r_x, r_y, c_1, \ldots, c_{h-1}, c_{h+1}, \ldots, c_m \in_R \mathbb{Z}_p$, and compute S_1 and S_2 as in (13) as follows:

$$\begin{aligned} S_1 &= g^{r_x} h^{r_y} \prod_{i=1, i\neq h}^{m} \left(\text{Key\_pub}_i\right)^{c_i}, \\ S_2 &= e^{r_x} \cdot \text{tag\_}R_p \cdot \left(\sum_{1\le i\le m,\ i\neq h} c_i\right). \end{aligned} \tag{13}$$

Step 3. Solve (14) to obtain c_h,

$$\begin{aligned} &\left(c_1 + \cdots + c_h + \cdots + c_m\right) \bmod p \\ &\quad = H'\left(t_s \| Y \| L\left(R_p\right) \| \text{tag\_}R_p \| M_1 \| S_1 \| S_2\right), \end{aligned} \tag{14}$$

where vector $Y = (\text{Key\_pub}_1, \text{Key\_pub}_2, \ldots, \text{Key\_pub}_m)^{\mathrm{T}}$ and Key_pub_i $(i = 1, \ldots, m)$ is the public key of R_i as setting in the system initializing.

Step 4. Output the signature

$$\begin{aligned} &\text{Sign\_}R_p\left(M_1\right) \\ &\quad = \left(\text{tag\_}R_p, t_s, L\left(R_p\right), x', y', c_1, \ldots, c_m\right), \end{aligned} \tag{15}$$

where $x' = (r_x - c_h \cdot x) \bmod p$, $y' = (r_y - c_h \cdot y) \bmod p$, and c_h is solved from (14).

After receiving $\text{Sign\_}R_p(M_1)$ from R_p, V_i will check the signature $\text{Sign\_}R_p(M_1)$, and the checking process is descripted in Algorithm 6. If the signature checking of $\text{Sign\_}R_p(M_1)$ is passed in Algorithm 6, V_i can obtain its temporal identity certificate as

$$\begin{aligned} \text{Id\_}V_i\left(R_p, t_s\right) &= M_1 \| \text{Sign\_}R_p\left(M_1\right) \| V_i\text{-pub}' \| \\ &\quad \text{Encrypt\_}V_i\text{-sec}\left(M_1 \| \text{Sign\_}R_p\left(M_1\right) \| V_i\text{-pub}'\right), \end{aligned} \tag{16}$$

where $V_i\text{-pub}'$ is another public key of V_i gotten from TA in the setting phase; that is, $V_i\text{-pub}' \in \{(V_i\text{-pub}_j, V_i\text{-sec}_j) \mid j = 1, 2, \ldots, k\}$.

Algorithm 6 (checking process of $\text{Sign\_}R_p(M_1)$).

Step 1. Compute $e = H(t_k)$.

Step 2. Abstract the value of $(\text{tag\_}R_p, x', y', c_1, \ldots, c_m)$ from $\text{Sign\_}R_p(M_1)$, and compute W_1, W_2, c_0 as follows:

$$\begin{aligned} W_1 &= g^{x'} h^{y'} \prod_{i=1}^{m} \text{Key\_pub}_i^{c_i}, \\ W_2 &= e^{x'} \cdot \text{tag\_}R_p^{(c_1+\cdots+c_m)}, \\ c_0 &= H'\left(t_s \| Y \| L\left(R_p\right) \| \text{tag\_}R_p \| M_1 \| W_1 \| W_2\right). \end{aligned} \tag{17}$$

Step 3. Checks whether (18) is satisfied,

$$c_0 \stackrel{?}{=} \left(\sum_{1\le i\le m} c_i\right) \bmod p. \tag{18}$$

If it is true, then pass; else V_i regards this round of protocol application as failure.

4.3.2. Temporal Identity Update. In VANETs, vehicles ask for authentication when driving in the area of a new RSU. This subsection considers the authentication process of a vehicle V_i coming from the area of R_p and joining in the area of R_q, and we let R_q update the identity certificate of V_i.

Figure 5 gives a concise description of the updating process of the temporal identity, and Protocol 7 gives detailed operation and computing process, where $\text{Id\_}V_i(R_p, t_s)$ was denoted in (16), M_1 was defined by (10), $\text{Sign\_}R_p(M_1)$ denotes message M_1 signed by R_p, and Algorithm 6 was presented in Section 4.3.1.

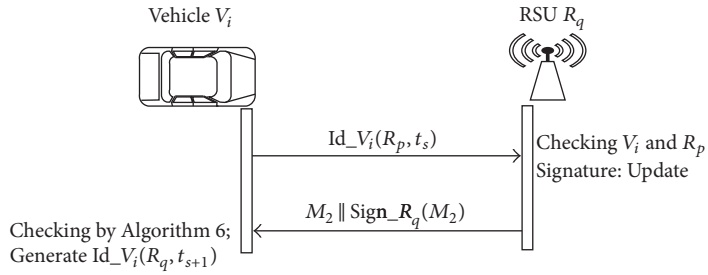


Figure 5: Update protocol of vehicle's temporal identity.

Protocol 7 (update protocol of vehicle's temporal identity).

Step 1. V_i send Id_$V_i(R_p, t_s)$ to R_q and request an update.

Step 2. R_q uses V_i-pub to authenticate Id_$V_i(R_p, t_s)$, then checking Sign_$R_p(M_1)$ according to Algorithm 6; if the authentication and checking are both passed, then generate M_2:

$$M_2 = \left(t_{s+1}, V_i\text{-pub}', L\left(R_p\right), L\left(R_q\right)\right), \tag{19}$$

R_q obtains Sign_$R_q(M_2)$ by using Algorithm 6 to sign on M_2 and sends $M_2 \parallel$ Sign_$R_q(M_2)$ to V_i.

Step 3. After receiving the message $M_2 \parallel$ Sign_$R_q(M_2)$, V_i uses Algorithm 6 to check it and generates his new identity certification:

$$\begin{aligned} \text{Id\_}V_i\left(R_q, t_{s+1}\right) = M_2 \parallel \text{Sign\_}R_q\left(M_2\right) \parallel V_i\text{-pub}''' \parallel \\ \text{Encrypt\_}V_i\text{-sec}'\left(M_1 \parallel \text{Sign\_}R_q\left(M_2\right) \parallel V_i\text{-pub}''\right), \end{aligned} \tag{20}$$

where V_i-pub$'' \in \{(V_i\text{-pub}_j, V_i\text{-sec}_j) \mid j = 1, 2, \ldots, k\}$.

In Figure 1, when a vehicle V_i calls for an identity update, it sends its current temporal identity Id_$V_i(R_p, t_s)$ to the nearest RUS, denoted as R_q, where R_p was the former RSU who signed the current identity and R_q is the RSU who will sign a new identity in this protocol. After receiving the application message from V_i, R_q starts the checking process as Step 2 in Protocol 7 and then generates and sends $M_2 \parallel$ Sign_$R_q(M_2)$ to V_i if the application message passes the checking. And V_i will obtain the new temporal identity Id_$V_i(R_q, t_{s+1})$ by Step 3 in Protocol 7.

4.4. Detection Method for Conspiracy Sybil Attack. Obtaining multiple legal identity is the basic and key step of Sybil attack; thus, we detect the abusing identity certificates to prevent the attack. In DMON, we employ multiple pairs of public key for vehicles and ring signature scheme of RSU as discussed in [10, 22]. The prevention of the abusing in multiple public key pairs or ring signature is also discussed in the related work [10, 22]. So we focus on conspiracy Sybil attack in this subsection.

In conspiracy Sybil attack, the conspired vehicles send their identity information to the attacker; thus, the attacker brings multiple certificate in travel. There are two situations: one is that the conspired vehicle comes along with the attacker; then we think it is not an attack for the identity certificate is always generated by the correct vehicle; another situation is that the conspired vehicles send their identity certificates to the attack far away from the attacker, and the attacker generates a new legal identity by passing the authentication of RSU and further update the certificate.

Theorem 8. *If an attacker V obtains the temporal identity certificate Id_$V_i(R_p, t_s)$ of a vehicle V_i, it cannot replace the signature information of R_p in Sign_$R_p(M_1)$, even if it gets the secret key of V_i.*

Proof. We assume that discrete logarithm problem is hard-solved. If an attacker fakes a new signature New_Sign_$R_p(M_1)$ to replace Sign_$R_p(M_1)$, according to Algorithm 5, it should make the parameters in New_Sign_$R_p(M_1)$ satisfy (13) and (14).

Assume that $K = g^{\beta} h^{\beta'}$, where $\beta, \beta' \in \mathbb{Z}_p$, if the attacker succeeds in faking the authentication message $(\text{tag}^i, t_s^i, L_i^i, x'^i, y'^i, c_1^i, \ldots, c_n^i)$, $i = 1, \ldots, n$, then we have a linear system of n equations as follows:

$$\beta = x'^i + c_1^i x_1 + \cdots + c_n^i x_n \quad i = 1, \ldots, n. \tag{21}$$

By the forking Lemma in [24], there is a chance that each successful rewind simulation is at most $(\epsilon/4)^n$, where ϵ is the probability that an attacker knows all the parameters, but the attacker did not know c_k. Hence, it is quite a small chance to forge New_Sign_$R_p(M_1)$. □

Theorem 9. *When a vehicle obtains a temporal certificate from R_p and updates the certificate in R_p by Protocol 7, if $L(R_p)^T \cdot L(R_q) \geq 2$, then R_p is in the 2-hop area of R_q.*

Sign_$R_p(M_1)$ and Sign_$R_q(M_2)$ cannot be replaced from Theorem 8. Then $L(R_p)$ and $L(R_q)$ cannot be altered, which are the label vectors contained in Sign_$R_p(M_1)$ and Sign_$R_q(M_2)$. According to the proof of Lemma 4, if $L(R_p)^{\mathrm{T}} \cdot L(R_q) \geq 2$, then there are at least 2 values of k, satisfying that $L_{ik} \neq 0$ and $L_{jk} \neq 0$, where $\text{Lab}_i \rightarrow R_p$ and $\text{Lab}_j \rightarrow R_q$. That is to say, R_p and R_q have 2 mutual neighbors RSU at least. Thus, R_p is the neighboror 2-hop neighbor of R_q.

We can conclude that the certificate of our DMON cannot be faked from Theorem 8, and the conspiracy identity certificate from 2-hop away will be detected by Theorem 8. As mentioned before, the conspiracy identity in the nearby

area and the abusing of multiple pseudonym will be detected by the scheme proposed in [10, 22], and we can directly use these schemes in DMON.

Now we will also limit the life period of the signature message of RSU, which will recognize the fresh identity from the certificates deliberately assembled by repeated signature. For example, in Figure 1, if V_A saves the used certificates those were obtained when it travels the routing just like V_1, V_2, and V_3 in the past. In this detection process, it can still use these old certificates with another pseudonym to cheat. Hence, we set a judgment condition in Algorithm 6 to check the freshness and validity of identity certificate:

$$t_s + \Delta t > t, \tag{22}$$

where time t_s belongs to time period $[t_k, t_{k+1}]$ and t is the current identification time which should belong to period $[t_{k+1}, t_{k+2}]$. In the meantime, the life period Δt in Sys_P should be carefully set: although a short life period could largely increase the detection rate, a longer period will permit a vehicle drive from a RSU to another and never need to apply a certificate in the same RSU.

5. Performance Analysis and Evaluation

Four objectives are given in designing DMON: detecting conspiracy Sybil attack, preserving privacy information (vehicles' ID and Location), achieving online and independent detection, and obtaining high efficiency and low overhead. Section 4.4 descripts the detection method, and Theorems 8 and 9 support online and independent detection. This section will evaluate the performance of proposed scheme in views of privacy leaking and computation overhead; thereafter, detection rates will be simulated.

5.1. Privacy Protection. Vehicles have two aspects of privacy, identity privacy and trajectory privacy. The ring signature scheme is employed in DMON ensuring the identity privacy. Trajectory privacy can be guaranteed by Theorem 10.

Theorem 10. *Attacker cannot obtain the vehicle's trajectory from the location of RSU included in the identity certificate defined by Algorithms 5 and 6 and Protocol 7.*

Proof. In Algorithm 5, a vehicle V_i will generate tag_$R_p = e^x$ when it drives in the area of a RSU, where x is abstracted from the random selected public key of V_i. Thus, RSU signs different messages for different vehicles, and the signature is unlinkable and untraceable. That is to say, the attacker cannot obtain the location and trajectory information from the signed certificate of RSU.

On the other hand, the identity certificate defined in (16) does not reveal any information of RSU in plain text. The label vector $L(R_p)$ contains the neighbor relationship, but the relationship was obfuscated and hidden by Figure 3, (4), (5), and (9). Unordered obfuscation and periodic update make the other RSUs and vehicle unable to catch the relation between $L(R_p)$ and R_p. Hence, the attacker cannot analyze the routing information from the label vector $L(R_p)$ contained in the signature of RSU. □

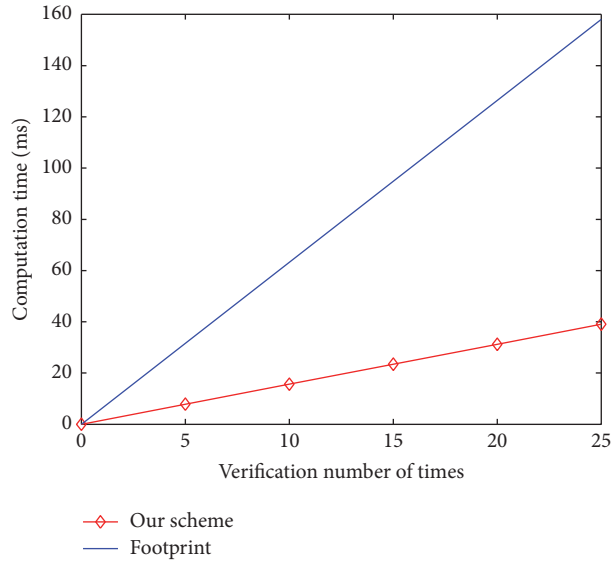


Figure 6: Computation cost of signature verification.

5.2. Computation Cost. There are four kinds of operations in the ring signature scheme. They are modular addition, modular multiplication, modular exponentiation, and secure cryptographic hash, denoted as *Add*, *Mul*, *Exp,* and *Hash*, respectively. Since the *Exp* and *Hash* operations are far more computationally expensive than the other two operations, so we only consider the number of Expand Hash operations to analyze the computational complexity of this scheme. We evaluate the computation cost of DMON as follows.

(1) Cost of Signing a Signature in Algorithm 5. Once a RSU joins in the system, it first gets the system parameter and computes e and tag_R_p. Then RSUs randomly choose parameters for signature, that is, $r_x, r_y, c_1, \ldots, c_{h-1}, c_{h+1}, \ldots, c_m$, and compute S_1 and S_2. The computed S_1 and S_2 are both multibases exponentiation. However, S_1, S_2, e, and tag_R_p can be used in the next signature after one-time computing until the certificate updates. Therefore, at most occasion, the RSU just computes the hash value c_m.

(2) Cost of Signature Verification in Algorithm 6. When a vehicle verifies a signature issued by a certain RSU, it should compute W_1, W_2, and c_0, where the cost of computing W_1 and W_2 are almost two multibases exponentiation. So we need two multibases exponentiation and one hash to verify the signature. We contrast the computation overhead of verification of DMON with Footprint [10] as shown in Figure 6.

5.3. Performance Simulation. MOVE [25] and SUMO [26] are used to configure experimental environments. The real world map is downloaded from TIGER database file, as showed in Figure 7. In this map, there are 383 points and 1,188 road segments in total.

In the simulation experiments, the traffic light is set to get more reliable results. In the situation of traffic congestion,

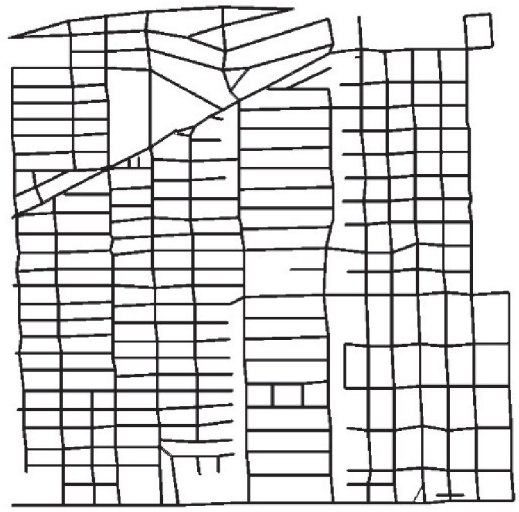


Figure 7: Real world map downloaded from TIGER.

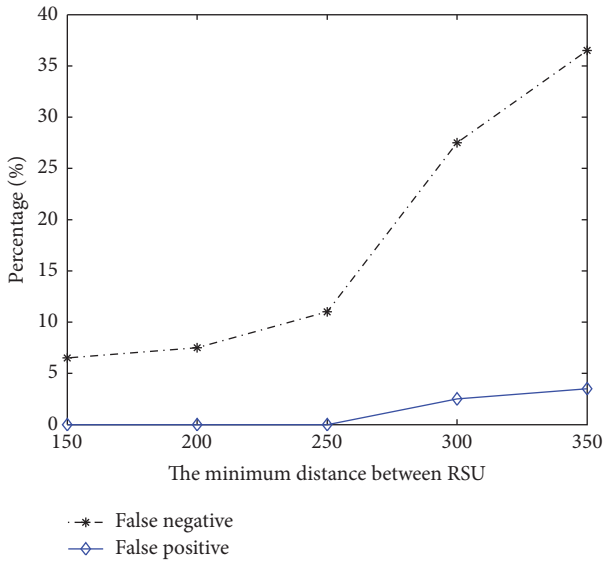


Figure 8: Influence of RSU distance.

vehicles would wait for a long time, but in a smooth traffic, a conspiracy vehicle might pass 2 or 3 RSUs in one minute. The number of Sybil attackers is set as the ratio $\rho = 10\%$ of all nodes. The attackers can independently launch a Sybil attack by the conspired ID, but the conspiracy vehicles are not involved in the attacks.

We first study the influence of RSU deployment in detection. In the experiment, we set the minimum distance between RSUs change from 150 meters to 350 meters; Figure 8 shows an obvious influence on the conspiracy Sybil attack detection, in which sparser RSU deployment would rapidly reduce the system performance. From Figure 8, we argue that 250 is a good minimum distance for RSU quantity which is not too large, and false positive error and false negative error are adoptable.

Then we simulate the life period Δt of vehicle identities to analyze its influence. We set the RSU in 2 steps. First, we deploy RSUs at the intersections which have large traffic volume. Then an RSU is deployed at an intersection if it is more than 250 meters away from the nearest deployed RSU, where 250 meters is a good value concluded from Figure 7. By this way, we deploy 100 RSUs in the map. We define that 2 RSUs are neighbors if the distance between them is less than 400 meters. As shown in Figure 9(a), 10 percent of vehicles are set as conspiracy vehicles in the simulation system; when Δt comes to 200 seconds, the false negative error increases in Figure 9(a). The reason is that attackers have enough time to obtain more valid conspiracy temporal identity certificates. Meanwhile, the false positive drops for the reason that legal vehicles would not be verified illegal for the life period when they collect more temporal identity certificates in their trajectory.

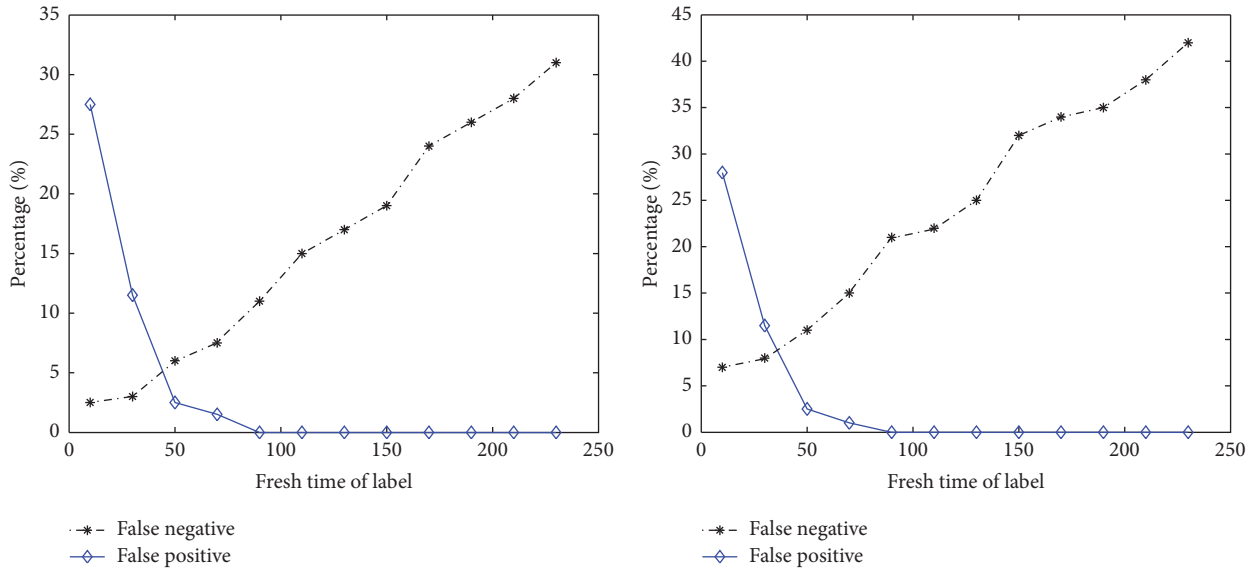
In Figure 9(b), we still set 10 percent of vehicles are conspired, but the conspiracy vehicles are randomly selected by the attacker. Then the false negative is a higher than that with static ones in Figure 9(a). The reason is that the mobility of vehicles is independent; an attacker will get more temporal identity certificate if it can choose the conspiracy vehicles nearby.

6. Conclusion

This paper focuses on a novel conspiracy Sybil attack which has main difference in obtaining Sybil identities from conspired vehicles. The forged identities are legal and cannot be detected by a general detection scheme. For this reason, a new detection scheme, named DMON, is proposed to detect conspiracy Sybil attack. DMON applies the signed certificate as the temporal identity of vehicles in VANETs and adopts the neighbor relationship of RSUs to detect faked identity. Meanwhile, an obfuscated label is presented to hide RSU's neighbor relationship with the purpose of preventing trajectory based privacy from leakage. DMON also has limitations in an assumption that indicates information synchronization of all RSUs in signature verification. The assumption is argued to be a little strong in practice, though the independent detection is realized through computing vector product in DMON. In future work, we will focus on identity authentication with local information only.

Notations

V_i:	The ith vehicles
R_i, R_p, R_q:	The ith, pth, qth RSU
G:	Group of prime order p
H:	Map to point function $H : \{0,1\}^* \to G$
H':	One-way hash function $H : \{0,1\}^* \to Z_p$
Δt:	Life period
t_s:	t_s belongs to time period $[t_k, t_{k+1}]$
$(\text{Key\_pub}_i, \text{Key\_sec}_i)$:	Public and secret key of R_i
$(V_i\text{\_pub}_j, V_i\text{\_sec}_j)$:	Public and secret key of V_i



(a) 10% conspiracy vehicles

(b) 10% vehicles will be chosen as conspiracy

FIGURE 9: Influence of life period Δt.

A_RSU: Neighbor relationship matrix of RSUs
PKL: The list of RSUs' public key
Sys_P: The public system parameters.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work is supported by the National Natural Science Foundation of China under Grants nos. 61472001 and 61272074. The authors would like to thank Master students Ya-li Shi and Wen-jun Wang for their constructive suggestions and helpful experiment skills.

References

[1] L. Wang, T. Li, and L. Chen, "Security issues and system structure of internet of vehicles," *Journal of Network and Information Security*, vol. 1, no. 22, pp. 41–54, 2016.

[2] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 7, pp. 3589–3603, 2010.

[3] C. Piro, C. Shields, and B. N. Levine, "Detecting the sybil attack in mobile Ad hoc networks," in *Proceedings of the IEEE/ACM International Conference on Security and Privacy in Communication Networks (SecureComm '06)*, pp. 1–11, Baltimore, Md, USA, September 2006.

[4] L. Zhang, D. Gao, and C. Foh, "A survey of abnormal traffic information detection and transmission mechanisms in VSNs," *International Journal of Distributed Sensor Networks*, vol. 10, no. 5, pp. 1–13, 2014.

[5] S. Abbas, M. Merabti, D. Llewellyn-Jones, and K. Kifayat, "Lightweight sybil attack detection in MANETs," *IEEE Systems Journal*, vol. 7, no. 2, pp. 236–248, 2013.

[6] B. Yu, C.-Z. Xu, and B. Xiao, "Detecting Sybil attacks in VANETs," *Journal of Parallel and Distributed Computing*, vol. 73, no. 6, pp. 746–756, 2013.

[7] P. Sarigiannidis, E. Karapistoli, and A. A. Economides, "Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information," *Expert Systems with Applications*, vol. 42, no. 21, pp. 7560–7572, 2015.

[8] N. Borisov, "Computational puzzles as sybil defenses," in *Proceedings of the Sixth IEEE International Conference on Peer-to-Peer Computing (P2P '06)*, pp. 171–176, Cambridge, UK.

[9] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "P2DAP—Sybil attacks detection in vehicular ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 582–594, 2011.

[10] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, "Footprint: detecting Sybil attacks in urban vehicular networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 6, pp. 1103–1114, 2012.

[11] B. Lee, E. Jeong, and I. Jung, "A DTSA (detection technique against a sybil attack) protocol using SKC (session key based certificate) on VANET," *International Journal of Security and its Applications*, vol. 7, no. 3, pp. 157–165, 2013.

[12] R. Hussain, H. Oh, and S. Kim, "AntiSybil: standing against Sybil attacks in privacy-preserved VANET," in *Proceedings of the 1st International Conference on Connected Vehicles and Expo (ICCVE '12)*, pp. 108–113, IEEE, Beijing, China, December 2012.

[13] X. Lin, "LSR: mitigating zero-day sybil vulnerability in privacy-preserving vehicular peer-to-peer networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 237–246, 2013.

[14] X. Feng, C.-Y. Li, D.-X. Chen, and J. Tang, "A method for defensing against multi-source Sybil attacks in VANET," *Peer-to-Peer Networking and Applications*, 2016.

[15] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," *ACM Computing Surveys*, vol. 42, no. 1, article no. 1, 2009.

[16] U. Khan and S. Agrawal, "Detection of Malicious Nodes (DMN) in vehicular ad-hoc networks," *Procedia Computer Science*, vol. 46, no. 9, pp. 965–972, 2015.

[17] X. Feng, C. Li, D. Chen, and J. Tang, "EBRS: event based reputation system for defensing multi-source sybil attacks in VANET," in *Proceedings of the 10th International Conference on Wireless Algorithms, Systems, and Applications (WASA '15)*, pp. 145–154, August 2015.

[18] K. Rabieh, M. M. E. A. Mahmoud, T. N. Guo, and M. Younis, "Cross-layer scheme for detecting large-scale colluding Sybil attack in VANETs," in *Proceedings of the IEEE International Conference on Communications (ICC '15)*, pp. 7298–7303, London, UK, June 2015.

[19] J. R. Douceur, "The sybil attack," in *Peer-to-Peer Systems*, vol. 2429 of *Lecture Notes in Computer Science*, pp. 251–260, Springer, Berlin, Germany, 2002.

[20] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: analysis & defenses," in *Proceedings of the Third International Symposium on Information Processing in Sensor Networks (IPSN '04)*, Berkeley, Calif, USA, April 2004.

[21] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against sybil attack in vehicular ad hoc network based on roadside unit support," in *Proceedings of the IEEE Military Communications Conference (MILCOM '09)*, pp. 1–7, Boston, Mass, USA, October 2009.

[22] J. K. Liu, M. H. Au, W. Susilo, and J. Zhou, "Linkable ring signature with unconditional anonymity," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 1, pp. 157–165, 2014.

[23] L. Chen, X. Jia, L. Meng, and L. Wang, "Expedite privacy-preserving emergency communication scheme for VANETs," *International Journal of Distributed Sensor Networks*, vol. 9, no. 5, pp. 1–13, 2013.

[24] D. Pointcheval and J. Stern, "Security proofs for signature schemes," in *International Conference on the Theory and Applications of Cryptographic Techniques EUROCRYPT 1996: Advances in Cryptology—EUROCRYPT '967*, pp. 387–398, Springer, Berlin, Germany, 1996.

[25] F. K. Karnadi, Z. H. Mo, and K.-C. Lan, "Rapid generation of realistic mobility models for VANET," in *Proceedings of the 2007 IEEE Wireless Communications and Networking Conference (WCNC '07)*, pp. 2508–2513, Hong Kong, March 2007.

[26] SUMO—Simulation of Urban Mobility, http://sumo.sourceforge.net.