Peer-to-Peer Netw. Appl. (2017) 10:305–314
DOI 10.1007/s12083-016-0431-x

# A method for defensing against multi-source Sybil attacks in VANET

**Xia Feng[1] · Chun-yan Li[2] · De-xin Chen[3] · Jin Tang[1]**

Received: 20 October 2015 / Accepted: 8 January 2016 / Published online: 29 January 2016


**Abstract** Sybil attack can counterfeit traffic scenario by sending false messages with multiple identities, which often causes traffic jams and even leads to vehicular accidents in vehicular ad hoc network (VANET). It is very difficult to be defended and detected, especially when it is launched by some conspired attackers using their legitimate identities. In this paper, we propose an event based reputation system (EBRS), in which dynamic reputation and trusted value for each event are employed to suppress the spread of false messages. EBRS can detect Sybil attack with fabricated identities and stolen identities in the process of communication, it also defends against the conspired Sybil attack since each event has a unique reputation value and trusted value. Meanwhile, we keep the vehicle identity in privacy. Simulation results show that EBRS is able to defend and detect multi-source Sybil attacks with high performances.

**Keywords** Vehicular ad hoc network · Multi-source Sybil attacks · Event reputation value · Event trusted value

✉ Xia Feng
fengx.ahu@foxmail.com

Chun-yan Li
lcy20110416@163.com

De-xin Chen
lhy5154@163.com

Jin Tang
ahhftang@qq.com

[1] Co-Innovation Center for Information Supply, Assurance Technology, Anhui University, Hefei 230601, People's Republic of China

[2] School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, People's Republic of China

[3] College of Computer Science, Sichuang University, Chengdu 610065, People's Republic of China

## 1 Introduction

As an important part of Intelligent Transportation System (ITS), VANET has been developed rapidly in the past twenty years. It purports to promote traffic management, improve road safety and the quality of people's travel experience [1]. In VANET, there are two communication models: vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) communication, as described in Fig. 1. Different from the Delay-tolerant networks [2–4], the characteristics of fast and dynamic topology, autonomous movement and the influence of traffic rules, road and weather conditions bring many security threats to VANET [5, 6]. To deal with these threats, many applications of VANET give each vehicle a unique identity, and take some security rules and methods with these identities.

A legitimate identity gives a license for vehicle to act as an internal node in VANET, but the identity-based security is vulnerable to Sybil attack. It was first proposed by Douceur [7] in the context of peer to peer networks. In Sybil attack, the malicious node will play the role of multiple distinct nodes to cheat the other vehicles, or destroy the security rules with its multiple identities which are illegally obtained by the way of forgery, theft or conspired sharing. Sybil attack may bring serious threats to VANET. For

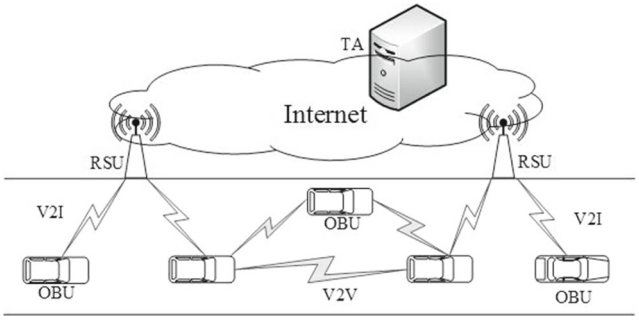


**Fig. 1** Architecture of VANET

example, sending false messages and fabricating traffic scenarios affect the normal travel [8]. In addition, Sybil attackers can destroy some vote-based routing protocols, change the voting results arbitrarily and even lead to DOS attacks to impair the normal operations of data dissemination protocols [9] with the multiple identities. In a word, Sybil attack will give the attackers many legitimate identities to do bad things, such as blackhole attack , wormhole attack and selective forwarding attack , replica attack [10–13], *etc*.

Currently, Sybil attack detection is an emerging research area in VANET. Many methods are proposed, such as RSSI-based (Received Signal Strength Indicator) detection method [14–16], vehicle movement trajectory based method [17, 18] and neighboring nodes information based method [19]. But there are two things that make the existing methods cannot work well: one is conspired Sybil attack, in which malicious vehicles obtain multiple false identities through the way of forgery, stolen and share their identities with the accomplices. The attackers have legitimate identities; the other is privacy requirement of anonymous [20, 21], that makes the impostors more difficult to be found.

In this paper we present an event based reputation system to defense Sybil attack, and we take multi-sources of false identity into account. In order to protect privacy, vehicle sends message with pseudonym instead of its real identity. Through verifying the local certificate of vehicle, EBRS can detect Sybil attack with forgery or theft identities. Moreover, in order to defense conspired Sybil attack, EBRS establishes a dynamic reputation value and trusted value for the event in VANET. If the reputation value and trusted value are below its corresponding threshold, the message about the event can't be spread, thus suppressing the propagation of false information. The rest of paper is organized as follows. In Section 2, a survey of existing Sybil attack detection methods is given. The models and design goals are given in Section 3. We propose EBRS in Section 4 and system evaluation in Section 5. Finally in Section 6, we conclude the paper and outline the future work.

## 2 Related work

Douceur [7] first described Sybil attack and proposed the resource testing (RT) method for Sybil attack in P2P networks. The main idea of this method is that every node in network is issued the same and limited resource such as computation resource, communication resource and storage capability. The verifier tests whether identities correspond to different nodes by verifying that each identity has as much of the tested resource as an independent node. As Sybil attacker need to allocate resource to its Sybil nodes, it can't have the same ability as normal node. However, the method of testing communication resource may cause channel congestion or even DOS attack. Moreover, resource testing is not applicable for VANET as the malicious vehicles may acquire multiple resource easily.

Newsome [22] established a taxonomy of different types of Sybil attack and proposed several novel methods such as radio resource testing (RRT), random key pre-distribution (RKPD) and code attestation (CA) to defend against Sybil attack in sensor network. Radio resource testing relies on the assumption that any node has only one radio which is incapable of sending or receiving on more than one channel simultaneously, which is unsuitable for ad hoc network. In random key pre-distribution, each sensor node is assigned a random set of keys or key-related information. The basic idea of code attestation is to exploit the fact that the code running on a malicious node must be different from that on a legitimate one. They are both not applicable for VANET as it may have large number of nodes.

SybilGuard (SybilG.) use social network to defend against Sybil attack [23–25]. Normal nodes will establish trust relationship with its neighbors quickly by communicating with them. However, Sybil attackers can have multiple false identities but it can't fabricate the trust relationship between Sybil nodes and honest nodes. Based on the fast mixing property of social networks, the method limits the corruptive influence of Sybil attacks. However, as vehicles move autonomously in VANET, the frequent changing topology brings a great challenge for using social network to defend against Sybil attack.

Assuming that every Sybil attacker is rational, it launches an attack only if its attack benefits are more than attack costs [26, 27]. The economy analysis method (EAM) can discourage the scale of Sybil attack while recurring fee may inhibits the initiative of normal nodes sending warning message to others.

As each vehicle has only one identity and one identity can't be located at two positions, each relatively accurate position has only one vehicle. Therefore, if the identity of a node and its position are bound together, we would be able to detect the Sybil attacks. Based on this idea, many

**Table 1** Comparison of related works, where S. is the abbreviation of static, 2S. indicates small scale, 3S. indicates static small scale network, W. is the abbreviation of wireless and MANET is the abbreviation of Mobile ad hoc network

| Detection methods | Applicable environment | Communication | | Identities | | Simultaneity | | Conspired Sybil attack |
|---|---|---|---|---|---|---|---|---|
| | | Direct | Indirect | Fabricated | Stolen | Simul. | Non-Simul. | |
| RT [4] | 2S. network | ✓ | ✓ | – | – | ✓ | × | N/A |
| RSSI [11] | W. network | ✓ | × | – | – | – | – | N/A |
| TSA [15] | MANET | ✓ | × | – | – | ✓ | × | N/A |
| SNI [16] | MANET | ✓ | ✓ | – | – | ✓ | × | N/A |
| RRT [19] | 3S. network | ✓ | × | ✓ | ✓ | ✓ | × | N/A |
| RKPD [19] | 3S. network | ✓ | × | – | – | ✓ | × | N/A |
| CA [19] | 2S. network | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| SyiblG. [20] | S. network | ✓ | × | – | – | × | × | N/A |
| EAM [23] | S. network | – | – | – | – | – | – | N/A |

✓ indicates the detection method can detect corresponding Sybil attack. × means that the detection method can't detect corresponding Sybil attack. – means that the detection method haven't nothing to do with that type of Sybil attack. N/A means that the method didn't consider that requirement

researchers proposed the method of estimating a node's position using RSSI to detect Sybil attack. If two messages have the same estimated position, we conclude that they are from the same node which is the Sybil attacker. Yu [14] estimated nodes positions using predetermined signal propagation model and RSSI to verify the accuracy of location information. A node is considered suspect if its claimed position is too far from the evaluated one. Bouassia [15] estimated the RSSI range of next message using Friis Free Space Path Loss Model [28]. If the real RSSI of next message is out of this range, we regard the sender is a Sybil vehicle. However, the message signal strength may be influenced by complex road conditions, so the detection accuracy is limited. What's more, this method can't defend against conspired Sybil attack. Taking the autonomous movement of vehicles into account, no vehicles will always pass by the same road side unit (RSU) at the same time in a certain period of time and an independent vehicle can't occur at different RSU at the same time. Therefore, taking RSUs as references, the vehicles generate their movement trajectories. Through computing and comparing vehicles' movement trajectories, Sybil attack can be detected. In urban VANET, there are fixed RSUs to provide extra service for vehicles. By receiving and saving the signatures which were broadcasted regularly by RSUs [17, 29] or actively requesting RSUs signatures [18] (also named as timestamp series approach, TSA), vehicles obtain movement trajectories. In V2V communications, vehicle has to send information with its motion information. Vehicles with the same or similar motion trajectory are Sybil attacker. However, this method has the risk of leaking out vehicles motion information and location privacy. Moreover, it can't resist Sybil attack with stolen movement trajectories and conspiracy Sybil attack.

Without consideration of traffic jam and vehicle fleet, different vehicles will not always have the same neighboring vehicles in a certain time period. Grover [19] put forward a method to detect Sybil attack using the similarity of neighboring information (SNI). Through exchanging and computing neighboring information between different vehicles, this method can detect Sybil attack. If some nodes observe that they have similar neighbors for a significant duration of time, these similar neighbors are identified as Sybil nodes. Although it doesn't need the help of RSU, the reality of neighboring information inter-vehicles depends on the loyalty of neighbor nodes. This can be used by the Sybil attackers to launch a new Sybil attack.

According to the applicable environment and Sybil attack taxonomy in [22] and the ability to defense against conspired Sybil attack, we make a comparison of the aforementioned Sybil attack detection methods in Table 1. We can see that most detection methods are not applicable for VANET for their impractical assumptions or high costs. RSSI-based method is applicable for all the wireless networks. However, it has difficulty in distinguishing Sybil nodes and normal nodes which are located near to each other. Vehicle movement trajectory based method has the risk of revealing vehicles location privacy. Neighboring nodes information based method has an assumption that the majority of neighbors are normal nodes which is a detection paradox itself. What's more, almost all the detection methods do not consider conspired Sybil attacks. In this paper, according to the false identity sources in Sybil attack and the characteristics of VANET, we propose an event based reputation system named EBRS which can protect vehicle privacy and defense

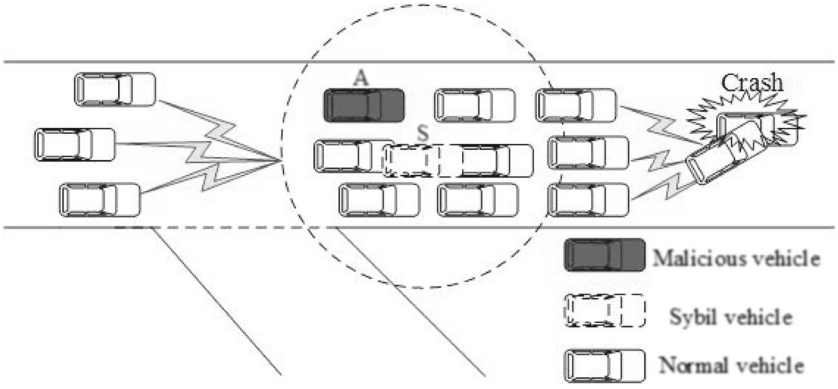


**Fig. 2** Faked smooth traffic scenario by Sybil attack

against Sybil attack with multi-sources.

## 3 Models and design goals

### 3.1 System model

Figure 1 illustrates the hierarchical architecture of VANET, which consists of three interoperating components. In VANET, each vehicle equips with an on board unit (OBU). It is used for real-time traffic information collection, traffic event perception, and warning messages acceptance. There is an event table (ET) to store different events and a tamper-proof device in OBU. RSU takes the role of a gateway between vehicles and TA. It will generate local certificates for vehicles in its communication range with an agreed session key. Government department is responsible for the role of trusted authority (TA). It takes charge of distributing and storing the nodes information in VANET. In this paper, we make the following assumptions. TA and RSU can never be compromised by any attackers and they are always trusted. The drivers can't tamper OBU information arbitrarily. The overlap area of RSUs is out of consideration of our work.

### 3.2 Attack model

To launch a Sybil attack successfully, a malicious node must try to present as multiple independent identities. It can fabricate traffic scenarios by sending false messages. Figure 2 shows the faked smooth traffic scenario launched by a Sybil attacker. Normally, vehicle will send warning message to notify other vehicles when it runs into traffic jam. Thus, other vehicles can slow down or detour to another road. However, Sybil attacker $A$ might create the illusion of a vehicle $S$ passing the traffic congestion area smoothly, $A$ has the legitimate identity and it can share its identity with the accomplices. Consequently, this action will impact the judgment of other drivers. They may make wrong decisions, leading the congestion area more congested or even vehicles pile-up. This is a great threat to the lives and properties of drivers and passengers. Similarly, in order to use the road itself, Sybil attackers can send false information in the situation of smooth traffic. In this work, we are intent to solve this Sybil attack related with sending false messages.

### 3.3 Design goals

To deal with the problems in existing Sybil attack detection methods and above attack model, we present an event based reputation system. Its design goals are:

- Conditional privacy preserving: vehicles use time-limited pseudonyms in the V2V and V2I communications which preserves the identity privacy of vehicles. But when a malicious vehicle is detected, TA has the ability to retrieve the vehicle's real identity from its pseudo identity. Therefore, EBRS can prevent the malicious node from repudiating its message.
- Independent detection: the essence of Sybil attack is collaboration of multiple Sybil nodes. To prevent the potential Sybil attack from happening again, the Sybil attack detection method should be carried by vehicles independently.
- Defense against Sybil attack with multiple false identity sources: Sybil attacker can get multiple false identities using the method of forgery, theft and conspiracy, EBRS is capable of defensing and detecting all theses Sybil attacks.

## 4 Event based reputation system

### 4.1 Initialization and notation

TA takes charge of the task of system initialization. According to the definition of bilinear maps, let $G_1$ be a cyclic

**Table 2** Notations

| Notations | Descriptions |
|---|---|
| $PID_v$ | Pseudonym of vehicle $v$ |
| $PK_v/sk_v$ | Public/secret key of vehicle $v$ |
| $PK_r/sk_r$ | Public/secret key of RSU $r$ |
| $Lcert_{rv}//Lcert_{vr}$ | Local certificate of vehicle $v$ in the range of RSU $r$ |
| $Cert_r$ | Certificate of RSU $r$ |
| $T$ | Fresh time of local certificate |
| $RV_E$ | Reputation value of event $E$ |
| $TV_E$ | Trusted value of event $E$ |
| $T_E$ | Time of event $E$ |
| $L_E$ | Location of event $E$ |
| $Type(E)$ | Type of event $E$ |

additive group which is generated by $P$ and $G_2$ be a cyclic multiplicative group. $G_1$ and $G_2$ have the same prime order $q$. $P$ is the generator and $P \in G_1$. TA chooses a random number $s$ as its prime secret key and it will update this key periodically. TA pre-distributes a unique ID, secret key, hash function $hash : \{0,1\}^* \longrightarrow Z_q^*$ and $s$ to the vehicle who wants to join in VANET. TA assigns a secret key and certificate to each RSU. The main notations throughout this paper are shown in Table 2.

### 4.2 EBRS process

EBRS establishes a local certificate for every vehicle and dynamic reputation value and trusted value for every event in VANET.

#### *4.2.1 Process of local certificate generation*

Before communicating with other nodes, a vehicle has to establish a local certificate with its local RSU. The process of local certificate generation is as follows, it can be depicted as Fig. 3.

1. According to elliptic curve cryptography (ECC) algorithm, vehicle $V_i$ obtains its public key $PK_i$ and pseudonym $PID_i$ through computing $PK_i = sk_i \cdot P \bmod n$ and $PID_i = hash(PK_i \| s)$. Then it sends $PK_i$ and $PID_i$ to its local RSU $r$.
2. After receiving the information, local RSU $r$ will store the information and send it to TA to validate $PK_i$ and $PID_i$.
3. If $PK_i$ or $PID_i$ has not passed TA verification, RSU $r$ will break off the process of local certificate generation forcibly. Otherwise, TA will send confirm information to RSU $r$. After receiving confirmation, RSU will compute its public key $PK_r$, session key $SK_{ri}$ with $V_i$ and $V_i's$ local certificate $Lcert_{ri}$ using the following formulas. After that, it will send $(PK_r, Cert_r, T)$ to $V_i$ and put $(PID_i, SK_{ri}, Lcert_{ri}, T)$ into its certificate list $(CL)$.

$$PK_r = sk_r \cdot P \bmod n \quad (1)$$

$$SK_{ri} = PK_r \oplus PK_i \bmod n \quad (2)$$

$$HV_{ri} = hash(PID_i || Cert_r) \quad (3)$$

$$Lcert_{ri} = HV_{ri} \times SK_{ri} \bmod n \quad (4)$$

4. After receiving the message from RSU $r$, $A$ will compute its session key $SK_{ir}$ with RSU $r$, $HV_{ir}$ and its local certificate $Lcert_{ir}$ using the following formulas. Under normal circumstances, $SK_{ir} = SK_{ri}, HV_{ir} = HV_{ri}, Lcert_{ir} = Lcert_{ri}$.

$$SK_{ir} = PK_i \oplus PK_r \bmod n \quad (5)$$

$$HV_{ir} = hash(PID_i || Cert_r) \quad (6)$$

$$Lcert_{ir} = HV_{ir} \times SK_{ir} \bmod n \quad (7)$$

#### *4.2.2 Process of local certificate validation*

After vehicle $V_i$ receives its local certificate, it can communicate with other vehicles. Assumed that there is a traffic accident in front of $V_i$, it will broadcast a warning message to its neighbors. The format of this message is $(PID_i, E_{SK_{ir}}(Lcert_{ir}), M, HM_i)$, where $M =$

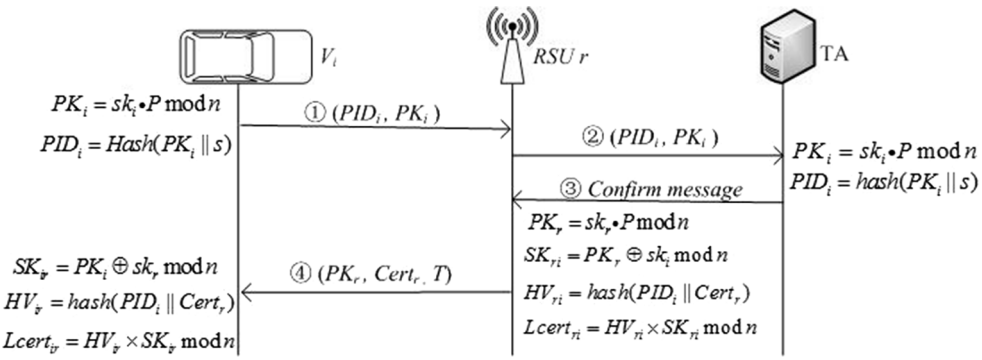


**Fig. 3** Process of local certificate generation

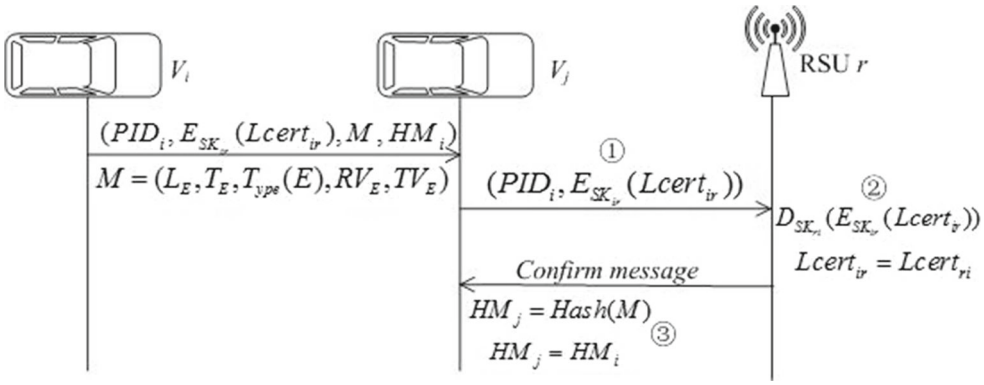


**Fig. 4** Process of local certificate validation

$(L_E, T_E, Type(E), RV_E, TV_E)$, $HM_i$ is the hash value of $M$. When vehicle $V_j$ (supposing it is in the range of $V_i$) receives the warning message from $V_i$, it has to validate if $V_i$ is a normal vehicle in VANET. The main process of validation is as follows, it can be formalized as Fig. 4.

1. $V_j$ will send $(PID_i, E_{SK_{ir}}(Lcert_{ir}))$ to its local RSU $r$ to authenticate the certificate of $V_i$.
2. RSU $r$ will search its $CL$ to get the session key with $V_i$ using $PID_i$. If formula 8 is satisfied and the certificate is within its fresh time $T$, the pseudonym and local certificate of $V_i$ is being proved to be correct. RSU $r$ will send the confirm message to $V_j$.

$$D_{SK_{ri}}(E_{SK_{ir}}(Lcert_{ir})) = Lcert_{ir} = Lcert_{ri} \tag{8}$$

3. Once receiving the confirmation message, $V_j$ will authenticate the integrity of message using formula 9. If it is satisfied, $V_j$ will record $RV_E$ and $TV_E$ or build an event entry in its ET. Otherwise, it will ignore the message from $V_i$.

$$HM_j = hash(M) = HM_i \tag{9}$$

There may be three reasons for the warning message not passing the validation of RSU. 1) $V_i$ attempts to use both expired pseudonym and certificate, with pseudonym and certificate in hand to communicate with other vehicles which leads to a Sybil attack; 2) A malicious node attempts to use the pseudonym stealing from $V_i$ to launch a Sybil attack but it doesn't get the session key of $V_i$ with RSU $r$; 3) A malicious vehicle attempts to launch Sybil attack by forging a pseudonym and session key. In this case, RSU $r$ will issue a warning message about Sybil attack and report to TA who can trace the malicious vehicle's real identity.

#### *4.2.3 Process of setting event reputation value and trusted value*

To deal with the problem of Sybil attack sending false messages, EBRS is enlightened by [30] to build a dynamic reputation value and trusted value for every event in VANET. Event reputation value is defined as the times of a vehicle sensing the event and the event trusted value is the number of distinct vehicles who have sensed the event. If vehicle $V_i$ senses an event $E_j$ for the first time, it will build an event entry for this event in its ET. At the same time, $V_i$ will broadcast a warning message to its neighbors. After receiving this warning message, $V_k$ (supposing it is in the range of $V_i$) will establish an event entry in its ET for this event if it hasn't sensed this event before. Otherwise, it will update the reputation value and trusted value of this event. When the reputation value and trusted value of this event both reach its corresponding threshold, $V_k$ will notify its driver through the user interface in OBU. The driver will take some actions about this event. Meanwhile, $V_k$ will broadcast a warning message about this event to its neighbors. If $V_i$ is a Sybil attacker who sends false message, its subsequent vehicles will not sense the event as it doesn't happen. Therefore, $RV_E$ and $TV_E$ will not reach their thresholds. Thus it inhibits the dissemination of false message. Supposing that $V_j$ is an accomplice of $V_i$, they plan to launch a Sybil attack. As they can't change $RV_E$, the event reputation value can't reach its threshold. Thus the false message

**Table 3** Simulation parameters

| Parameters | Values |
|---|---|
| Simulation time | $500s$ |
| Vehicles velocity | $10m/s - 30m/s$ |
| Communication range | $300m$ |
| MAC protocol | $802.11p$ |
| Sending frequency | 1 per second |

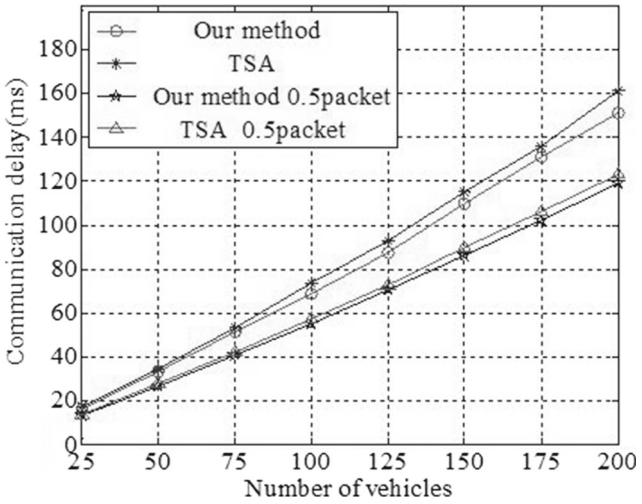


**Fig. 5** Communication delay

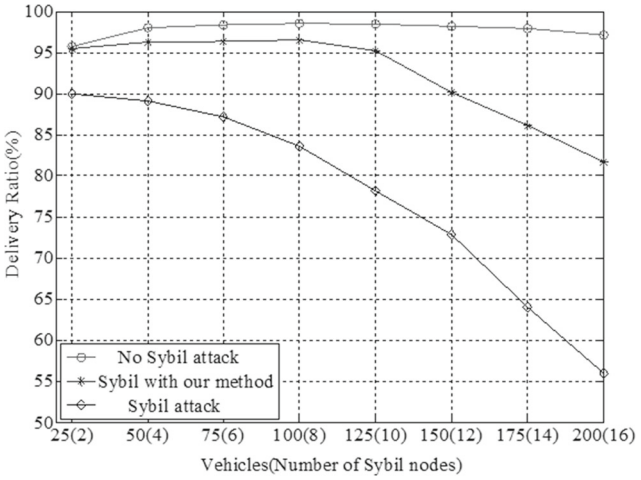


**Fig. 7** Delivery ratio in different conditions

will not be spread any longer, EBRS defends against the conspired Sybil attack. In Sybil attack with stolen identities, although the Sybil attacker can send false message with legitimate identity, the false message can't be spread any longer as the event reputation value and trusted valued can't reach their thresholds. In order to respond and transmit the message quickly which is very perilous and urgent, we can define different threshold for different type of event.

## 5 System evaluation

In this section, we analyze and evaluate the performance of EBRS. In our simulation, vehicles move according to the street map in the Houston area based on a Tiger database file. In this map, there are 383 points and 1,188 road segments in total. We have evaluated our method in 2 km road segment area obtained from these realistic traces with variation the number of vehicles. The simulation is based on NS2 which is an object-oriented, time-discrete network simulation tool. It can present many well-developed low-layer protocols with its easy programming interfaces. The simulation parameter is shown in Table 3.

### 5.1 Simulation results analysis

Figure 5 is the communication delay of EBRS and TSA with different packet size, 1 packet and 0.5 packet respectively, from which we can conclude that the communication delay of EBRS is much less than TSA. With the increase of vehicle density, the communication delay will increase. This is because that too many vehicles on the road will cause intense competition of wireless channel in the process of

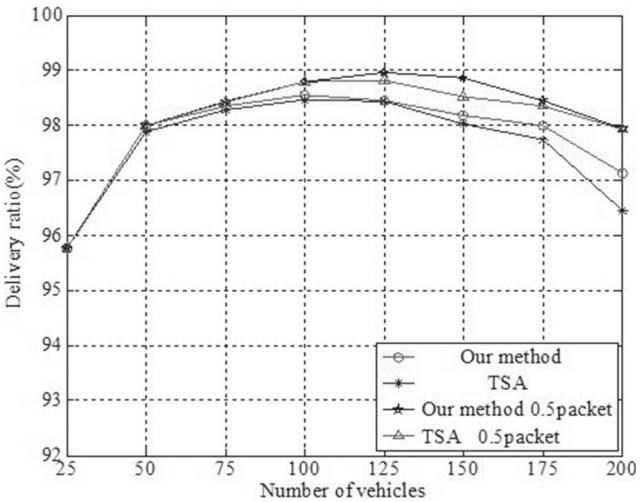


**Fig. 6** Delivery ratio

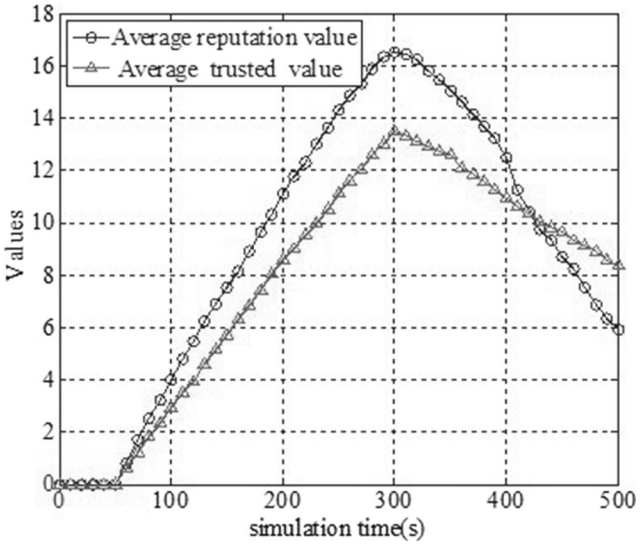


**Fig. 8** Average event reputation value and event trusted value

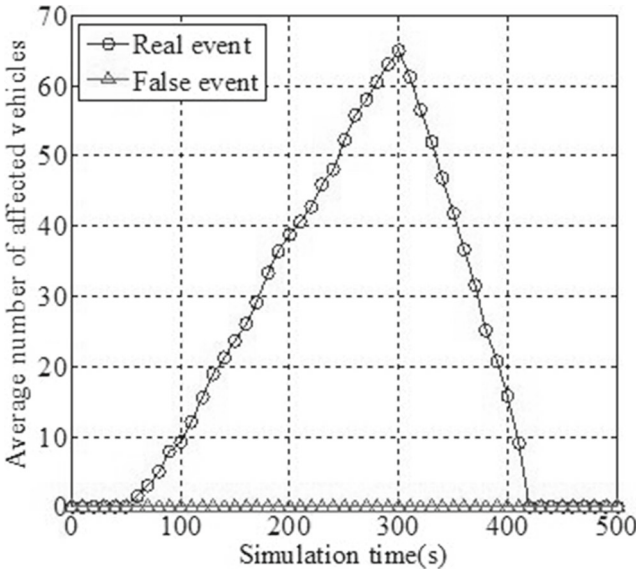


**Fig. 9** Average number of affected vehicles by false event and real event

communication. In addition, the bigger the packet is, the higher will be the communication delay. The delivery ratio of EBRS and TSA is shown by Fig. 6. It indicates that when the vehicle density is small, the message delivery ratio is small, too. The reason is that when the number of vehicles on the road is little, the distance between vehicles will be too far to receive the message. With the increase of node density, the delivery ratio will increase, too. But when the number of vehicles is above 100, the delivery ratio will be decreased. As more vehicles on the road, they will send message at the same time which leads to the increase of packets loss. From these figures, we can conclude that our method is much better than TSA.

We have made a simulation to study the influence of Sybil attack to the packet delivery ratio in VANET. At the same time, the effect of our method against Sybil attack is also studied. From Fig. 7, we can see that our method has good effect to reduce the impact of Sybil attack. The reason is that in our method, Sybil attack can be defended by the process of local certificate generation and validation. What's more, the false events sent by Sybil attackers can be prevented to transmit to normal vehicles. While in VANET without Sybil attack detection or defense method, the delivery ratio falls sharply. Therefore, it is very necessary to study the method to deal with Sybil attack.

To study the impact of event reputation value and event trusted value on EBRS, Fig. 8 shows the event reputation value and trusted value with the increase of simulation time. We suppose that the sampling interval of OBU is 1 s and range of sensor is 20 m. The event of traffic jam is happened at the $50th$ s. If the event reputation value doesn't change in 10 s, it will be decreased 1 per 20 s. When the event reputation value is 0, it will be deleted from the event table. As is shown in Fig. 9, the event reputation value and trusted value increases with the simulation time from the $50th$ to the $300th$ s. When the event is resolved at the $300th$ s, the corresponding values will decrease. We set the reputation threshold to 10 and trust value threshold to 4 of traffic jam. A vehicle trusting the existence of an event is defined as an affected vehicle. If there is a conspired Sybil attack in VANET, the malicious node will send false event to its neighbors. From Fig. 9, we can conclude that EBRS can prevent the spread of false event successfully. On the contrary, the real event can be spread quickly to many vehicles. As a result, EBRS defends against the conspired Sybil attack sending false message.

### 5.2 Performance evaluation

Table 4 gives the comparison of our method and some related work in Section 2. It indicates that our method can not only preserve vehicle privacy, guarantee message integrity, but also can defense against Sybil attack with multiple false identity sources. The marks in this table have the same meaning with Table 1.

The comparison of V2V communication overhead and V2I communication overhead of TSA and our method is given in Fig. 10. In TSA, not only message, but also the latest timestamp certificate and RSU certificate are needed to be concluded in the communication packet. Therefore, the communication overhead of TSA is much bigger than

**Table 4** Comparison of our method and other methods

| Detection methods | Sybil attack with fabricated identities | Sybil attack with stolen identities | Conspired Sybil attack | Message integrity | Privacy protection |
|---|---|---|---|---|---|
| RSSI [11] | – | – | N/A | N/A | N/A |
| TSA [15] | – | – | N/A | ✓ | × |
| SNI [16] | – | – | N/A | N/A | × |
| Our method | ✓ | ✓ | ✓ | ✓ | ✓ |

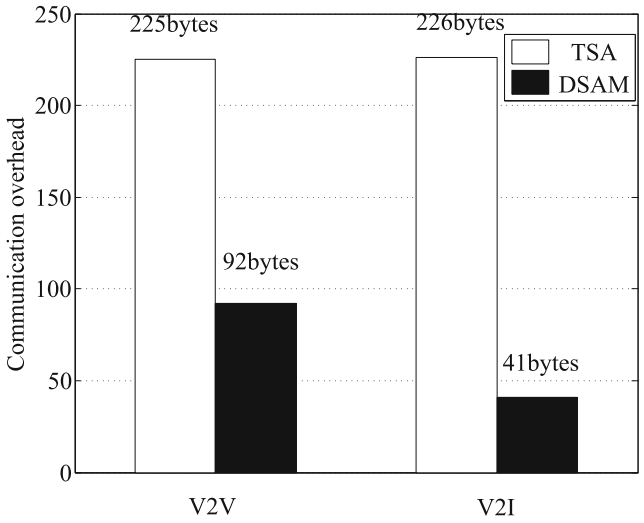


**Fig. 10** Comparison of communication overhead

our method. Assume that the length of message in two methods is 20 bytes. The traffic message length of V2V communication in TSA is $len(TM_1)$ and the V2V communication overhead in our method is $len(TM_2)$. They can be computed as follows.

$$\begin{aligned} &len(TM_1) \\ &= len(m) + len(Sig) + len(Cert\_T) + len(Cert\_R) \\ &= 20 \text{ bytes } + 28 \text{ bytes } + 107 \text{ bytes } + 70 \text{ bytes} \\ &= 225 \text{ bytes.} \end{aligned} \tag{10}$$

$$\begin{aligned} &len(TM_2) \\ &= len(m) + len(PID) + len(Enc) + len(hash) \\ &= 20 \text{ bytes } + 20 \text{ bytes } + 32 \text{ bytes } + 20 \text{ bytes} \\ &= 92 \text{ bytes.} \end{aligned} \tag{11}$$

When passing by RSU, each vehicle needs to request a new timestamp certificate. The length of requesting message in TSA is $len(Req_1)$:

$$\begin{aligned} &len(Req_1) \\ &= len(PK) + len(Sig) + len(Cert\_T) + len(Cert\_R) \\ &= 21 \text{ bytes } + 28 \text{ bytes } + 107 \text{ bytes } + 70 \text{ bytes} \\ &= 226 \text{ bytes.} \end{aligned} \tag{12}$$

Vehicle in EBRS only needs to send its pseudonym and public key to request a new certificate. The V2I communication overhead in EBRS is $len(Req_2)$:

$$\begin{aligned} len(Req_2) &= len(PID) + len(PK) \\ &= 20 \text{ bytes } + 21 \text{ bytes} \\ &= 41 \text{ bytes.} \end{aligned} \tag{13}$$

## 6 Conclusion and future work

Compared to existing methods, EBRS can defense against multi-source Sybil attacks, ensure the integrity of message and preserve the privacy of vehicles. By establishing a reputation threshold and trust threshold for each event message, the dissemination of false message is restricted no matter it is from forgery identities or legitimate identities. In EBRS, a trusted RSU is used to issue the certificate of vehicles in its communication range. Our further work will loosen the strong security assumption of RSU, and try to find an automatic mode to establish the trust relationship among the participant vehicles.

**Acknowledgments** This research was financially supported by National Natural Science Foundation of China under Grant An No.61472001 and No.U1405255, as well as the project of academic leaders funding of Anhui University under No.02303203. We would like to thank the anonymous reviewers for their insightful comments and suggestions.



## References

1. Al-Sultan S, Al-Doori MM, Al-Bayatti AH (2014) A comprehensive survey on vehicular Ad Hoc network. J Netw Comput Appl 37:380–392
2. Zhu H, Lin X, Lu R (2009) Smart: a secure multilayer credit-based incentive scheme for delay-tolerant networks. IEEE Trans Veh Technol 58:4628–4639
3. Zhu H, Du S, Gao Z (2014) A probabilistic misbehavior detection scheme toward efficient trust establishment in delay-tolerant networks. IEEE Trans Parallel Distrib Syst 25:22–32
4. Du S, Zhu H, Li X (2013) MixZone in motion: achieving dynamically cooperative location privacy protection in delay-tolerant networks. IEEE Trans Veh Technol 62:4565–4575
5. Sumra IA, Hasbullah HB, AbManan JB (2015) Attacks on security goals (confidentiality, integrity, availability). In: VANET: a survey. vehicular ad-hoc networks for smart cities. Singapore, pp 51–61
6. Wang LM, Li XJ, Zhong H (2013) A revocable group batch verification scheme for VANET. Science China: Information Science 43:1307–1325
7. Douceur JR (2002) The Sybil attack. In: Proceeding of international workshop on peer-to-peer systems. Cambridge, pp 251–260

8. Bissmeyer N, Stresing C, Bayarou KM (2010) Intrusion detection in VANETs through verification of vehicle movement data. Vehicular Networking Conference (VNC) 2010. IEEE press, New Jersey, pp 166–173
9. Zhao J, Cao G (2008) VADD: vehicle-assisted data delivery in vehicular ad hoc networks. IEEE Trans Veh Technol 57:1910–1922
10. Wang LM, Shi Y (2011) l Patrol detection for replica attacks on wireless sensor networks. Sensors 11:2496–2504
11. Park J, Seong D, Yeo M (2013) An energy-efficient selective forwarding attack detection scheme using lazy detection in wireless sensor networks. Ubiquitous information technologies and applications. Springer, Netherlands, pp 157–164
12. Bibhu V, Roshan K, Singh KB (2012) Performance analysis of black hole attack in VANET. Int J Comput Netw Inf Secur 4:47–54
13. Safi SM, Movaghar A, Mohammadizadeh M (2009) A novel approach for avoiding wormhole attacks in VANET. In: First Asian Himalayas international conference on internet, AH-ICI 2009. Kathmandu, Nepal. IEEE, pp 1–6
14. Yu B, Xu CZ, Xiao B (2013) Detecting Sybil attacks in VANETs. J Parallel Distrib Comput 73:746–756
15. Bouassida MS, Guette G, Shawky M (2009) Sybil nodes detection based on received signal strength variations within VANET. IJ Netw Secur 9:22–33
16. Guette G, Ducourthial B (2007) On the Sybil attack detection in VANET. In: IEEE International conference on mobile Ad hoc and sensor systems, MASS 2007. Pisa, Italy. IEEE, pp 1–6
17. Chen C, Wang X, Han WL (2009) A robust detection of the Sybil attack in urban VANETs. In: The 29th IEEE International conference on distributed computing systems workshops, ICDCS 2009. IEEE press, Montreal, pp 270–276
18. Park S, Aslam B, Turgut D (2013) Defense against Sybil attack in the initial deployment stage of vehicular ad hoc network based on roadside unit support. Secur Commun Netw 6:523–538
19. Grover J, Laxmi V, Gaur MS (2014) Sybil attack detection in VANET using neighbouring vehicles. Int J Secur Netw 9:222–233
20. Li Z, Chigan C (2014) On joint privacy and reputation assurance for vehicular Ad Hoc networks. IEEE Trans Mob Comput 13:2334–2344
21. Chim TW, Yiu SM, Hui LCK (2014) VSPN: VANET-based secure and privacy-preserving navigation. IEEE Trans Comput 63:510–524
22. Newsome J, Shi E, Song D (2004) The Slybil attack in sensor networks: analysis & defenses. In: Proceedings of the third international symposium on information processing in sensor networks. Berkeley, California, USA: ACM, pp 259–268
23. Yu H, Kaminsky M, Gibbons PB (2008) SybilGuard: defending against Sybil attacks via social networks. IEEE/ACM Trans Networking 16:576–589
24. Danezis G, Mittal P (2009) SybilInfer: detecting Sybil nodes using social networks. In: Proceedings of the network and distributed system security symposium. San Diego, California, USA, pp 1–15
25. Mohaisen A, Hollenbeck S (2014) Improving social network-based sybil defenses by rewiring and augmenting social graphs. Information security applications. Springer International Publishing, pp 65–80
26. Margolin NB, Levine BN (2008) Quantifying resistance to the Sybil attack. In: Financial cryptography and data security. Springer, Berlin, Heidelberg, pp 1–15
27. Bissias G, Ozisik AP, Levine BN (2014) Sybil-resistant mixing for bitcoin. In: Proceedings of the 13th workshop on privacy in the electronic society. ACM, pp 149–158
28. Friis HT (1946) A note on a simple transmission formula. Proc of IRE 34:254–256
29. Chang S, Qi Y, Zhu HZ (2012) Footprint: detecting Sybil attacks in urban vehicular networks. IEEE Trans Parallel Distrib Syst 23:1103–1114
30. Lo NW, Tsai HC (2009) A reputation system for traffic safety event on vehicular ad hoc networks. EURASIP J Wirel Commun Netw 2009:1–10