International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.4., 2015
(July-Aug)

REVIEW ARTICLE

ISSN: 2321-7758

SYBIL ATTACK DETECTION TECHNIQUE FOR VANETS: A NOVEL SCHEME

S.BHUVANESHWARI[1], Dr. V. PALANISAMY[2]
[1]M.Phil Scholar , [2]Professor and Head
Department of Computer Science and Engineering
Alagappa University, Karaikudi

ISSN:2321-7758
International Journal of Engineering Research-Online
A peer-reviewed, open access International scientific journal
www.ijoer.in

ABSTRACT

Vehicle adhoc networks (VANET) are an application of Mobile adhoc networks (MANET). VANET performs management of traffic very well. It also circulates safety information to drivers and passengers in the vehicle. Here, in this paper we have proposed a novel scheme of Sybil attack detection mechanism or algorithm by using which the trajectory path communication among vehicles for identification while still preserving their location details. When a vehicle comes within the communicable area of a road-side unit (RSU), it always demands an authorized message from the RSU as the proof of the appearance time at this RSU. The Sybil defense algorithm detects fake nodes from normal nodes in vehicular communication to avoid congestion.

I. INTRODUCTION

In recent years with the advancement of wireless technology VANETs have gained a lot of attention from industry and educational sectors. VANET is an emerging technology to increase road safety, efficiency and convenience. The mobile and dynamic topology of VANETs have created some challenging issues which are still unresolved. Dedicated Short Range Communications (DSRC) enables both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) applications. In this paper we focus on V2I and V2V communication. Vehicles can access Internet for various multimedia and intelligent transportation services while driving within the communication range of roadside unit (RSU).

Many VANET applications are location dependent, V2V and V2I communications are broadcast in nature, network connectivity is intermittent and vehicles often have high but predictable mobility. Considering these properties, simply implementing the existing IEEE 802.11i security standard and online certificate authority (CA)-based authentication schemes for VANET may not be desirable or feasible. In an insecure network to safeguard information exchange and to authenticate the entities VANET application requires security assurance. Key agreement protocol is a fundamental building block in securing VANETs. To ensure data confidentiality and integrity the key agreement protocols allow entities to implement key agreement and share the session key known to them alone. Trustful authentication is achieved in broadcast and high contention environments using these protocols.

Certificate less key agreement schemes for V2I communication assumes that the message from RSUs or vehicles can be relayed to locations outside their direct communication range. The RSU piggybacks security session parameters in its periodical beacon messages, and vehicles that are interested in accessing the RSU can relay the message to locations further away from RSU. During the relay process, the relayer adds its identity to the relayed message, so the receiver has the knowledge about the path of the relayed message. To access the services of RSU, a vehicle sends a reply message, which is relayed back to RSU. The relayer may aggregate the reply messages from others and its own whenever possible to reduce overhead.

The rest of this paper is organized as follows, Section 2 discusses the literature survey. Section 3 describes the VANET system model. Section 4 overviews about various attacks in VANET, Sybil attack detection approaches and DSDV protocol. Section 5 presents Sybil defence algorithm design. Performance results are given in Section 6, followed by further discussions and conclusions in Section 7.

II. Literature Review

In the literature review many Sybil attack detection techniques for VANET communication has been reviewed. They are as follows.

While it was first described and formalized by Douceur, the Sybil attack has been a severe and pervasive problem in many forms. In a Sybil attack, an attacker can launch a Sybil attack by forging multiple identifies, gaining a disproportionately large influence. In the literature, there have been many different approaches proposed to detect or mitigate the attack.

Many studies have followed Douceur's approach, focusing on how to establish trust between participating entities based on trusted public key cryptographies or certificates in distributed systems, for example, P2P systems, sensor networks and mobile ad hoc networks.

Although deploying trusted certificates is the only approach that has the potential to completely eliminate Sybil attacks, it also violates both anonymity and location has the problem of key revocation which is challenging, particularly in wireless mobile networks.

Another category of Sybil attack detection schemes is based on resource testing. The goal of resource testing is to determine if a number of identities possess fewer resources than would be expected if they were independent. The resources being tested can be computing ability, storage ability, and network bandwidth, as well as IP addresses. These schemes assume that entities have homogeneous hardware configurations. In vehicular networks, this assumption cannot hold since malicious vehicles can easily have more powerful resources than the normal vehicles.

Sybil Guard is an interesting scheme studying the social network among entities. In this scheme, human established real-world trust relationship among users is used for detecting Sybil attacks. Since even the attacker can generate as many as Sybil identities, building relationship between honest users and Sybil identities is much harder. Thus, there exists a small "cut" on the graph of trust relationship between the forged identities and the real ones. This is because vehicles are highly mobile. Communications often happen among temporarily met and unfamiliar vehicles.

To exploit the fact that one single vehicle cannot present at multiple locations at the same time, Bouassida have proposed a detection mechanism utilizing localization technique based on Received Signal Strength Indication (RSSI). In this scheme, by successively measuring the RSSI variations, the relative locations among vehicles in vicinity can be estimated. Identities with the same estimated locations are considered as Sybil vehicles. In practice, the complicated outdoor environments can dramatically affect the wireless signal propagation so that RSSI measurements are highly time variant even measured at the same location.

Xiao have proposed a Sybil attack detection scheme where the location of a particular vehicle can be determined by the RSSI measurements taken at other participating vehicles. 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. It is infeasible in practice due to the prohibitive cost. Furthermore, in such a scheme, vehicles should managed by a centralized trusted enter. 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.

The most relevant work to Footprint is the Sybil attack detection schemes proposed in. In these schemes, a number of location information reports about a vehicle are required for identification. 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. Trajectories made up of consecutive time stamps and the corresponding public keys of RSUs are used for identification. However, these schemes did not take location privacy into consideration since RSUs use long term identities to generate signatures. As a result, the location information of a vehicle can be inferred from the RSU signatures it collects. In Footprint, authorized messages issued from RSUs are signer-ambiguous which means the information about the location where the authorized message was issued is concealed, and temporarily linkable which means using a single trajectory for long term identification of a vehicle is prohibited. Therefore, the privacy of location information and identity of vehicles are preserved in Footprint.

A lightweight certificate less and one round agreement scheme without pairing, in the random oracle model resists known attacks with less computation cost and relieves the workload of vehicle to vehicle communication during the unavailable infrastructure circumstance as given in [1]

A novel privacy – preserving data forwarding scheme based on novel Lite - CA based public key cryptography and on path onion encryption technique. This scheme thwarts the traffic tracking attack at the minimized computational overhead and provides an efficient way to relieve workload and deployment complexity of certificates as well. This scheme is suitable for service oriented VANETs as discussed in [2]

A scheme for vehicles to upload to roadside units, called drive-thru internet, in a secure and efficient manner is discussed. Traditional certificate based security scheme are infeasible due to ad hoc nature and wireless communications. So they have used a certificateless approach to secure upload in a drive-thru internet. They have also discussed about various attack models and the means to solve this attack by certificateless scheme as explained in [3]

A model for certificateless authenticated key exchange (CL-AKE) protocols. The combination of an ID-based AKE protocol with a public key based AKE protocol cannot provide strong security. They provide the first one round CL-AKE scheme proven secure in the random oracle model. This scheme is secure even if the key generation centre learns the ephemeral secrets of both parties. This scheme is secure as long as each party has at least one uncompromised secret as given in [4]

The literature on certificateless encryption schemes is discussed. By ranking the notions of security for a certificateless encryption schemes against an outside attacker and a passive key generation centre and they have suggested which of these notions can be regarded as correct model for a secure certificateless encryption scheme. They have examined security models that aim to provide security against an actively malicious key generation centre. They have also surveyed the existing certificateless encryption scheme and compare their security proofs as given in [6]

A cryptographic scheme, which enables any pair of users to communicate securely and to verify each other's signatures without exchanging private or public keys, without keeping key directories, and without using the services of a third party as discussed in [7]

A short signature scheme is proposed based on the Computational Diffie-Hellman assumption on certain elliptic and hyper-elliptic curves. The signature length is half the size of a DSA signature for a similar level of security. Our short signature scheme is designed for systems where signatures are typed in by a human or signatures are sent over a low-bandwidth channel as explained in [8]

An efficient and spontaneous privacy-preserving protocol for vehicular ad-hoc networks based on revocable ring signature is introduced. The proposed protocol has three appealing characteristics: First, it offers *conditional privacy preservation*: while a receiver can verify that a message issuer is an authorized participant in the system only a trusted authority can reveal the true identity of a message sender. Second, it is *spontaneous*: safety messages can be authenticated locally, without support from the roadside units or contacting other vehicles. Third, it is *efficient*: it offers fast message authentication and verification, cost-effective identity tracking in case of a dispute, and has low storage requirements. We use extensive analysis to demonstrate the merits of the proposed protocol and to compare it with previously proposed solutions as given in [9]

An efficient conditional privacy preservation (ECPP) protocol in vehicular ad hoc networks (VANETs) to address the issue on anonymous authentication for safety messages with authority traceability. The proposed protocol is characterized by the generation of on-the-fly short-time anonymous keys between On-Board Units (OBUs) and Roadside Units (RSUs), which can provide fast anonymous authentication and privacy tracking while minimizing the required storage for short-time anonymous keys as in [2]

The main challenge with infrastructure-less network is developing communications and protocols that can deliver robust and reliable ad hoc communications between vehicles, when the relative speed is high under opposite traffic conditions. A solution for this opposite direction effect, by minimizing the effect of opposite traffic on routing packets. A router direction index is used to enhance the performance of ad hoc on demand distance vector protocol and a new queue priority mechanism is also used. The results obtained demonstrate a performance increase in the average data good put and less routing overhead for the proposed solution as explained in [3]

III. VANET System Model

The system model of VANETs consists of three components. They are Regional Trusted Authority (RTA), On Board Unit (OBU), Road Side Unit (RSU).

1.) RTA: There is only one trusted RTA in each vehicular network. RTA is powered with sufficient computation and storage capability. RTA has two main functions:
    - It computes the master key for the key agreement and publishes the requisite public parameters.
    - RTA controls the registration process of vehicles and computes pseudonym for vehicles when vehicles come into the communication range.

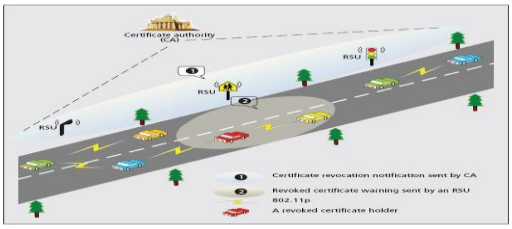
Certificate authority (CA)
1
RSU
RSU
2
RSU
1
Certificate revocation notification sent by CA
2
Revoked certificate warning sent by an RSU
802.11p
A revoked certificate holder

Figure 1. VANET System model

2.) OBU: is deployed on the vehicles as a trusted platform module (TPM). OBUs mainly communicate with each other for sharing local traffic information to improve the whole safety driving conditions, and with RSUs for requesting the short-time anonymous public key certificate. OBUs can communicate with RSUs through wireless channel. OBUs should register to RTA and obtain key materials in advance. Before OBUs communicate with each other, they exchange public keys and compute the session keys for encrypting the subsequent messages.

3.) RSU: RSUs are subordinated by the RTA, which holds storage units to store information from the TA and the OBUs. RSU is a trusted roadside unit which connects with RTA through wired channel and communicates with OBU via wireless channel; meanwhile, it has a wireless Access Point (AP) for all OBUs in its communication range. RSUs have two roles, data warehouse and processing centre authorized by the CA. So RSUs are important to act as the secure proxy between RTA and OBU. The main tasks of RSUs are
    1.) Issuing a short time anonymous public key certificate to each OBU when the OBU requests.
    2.) Assisting the RTA to efficiently track the real OBU identity of any safety message.

They are generally deployed in an optimized way for high utilization due to their high cost. Therefore, once the RSUs are unavailable in some areas, the V2I communications will be invalid or infeasible.

IV. CLASSIFICATION OF VANET ATTACKS

Because of the open nature of VANET they are vulnerable to various types of attacks. Attackers also categorizes as inside attacker and outside attacker. Some of the attacks which may impair VANET are as follows

1. Denial of Service attack

This type of attack can be carried out by network insider or outsider. In this attack an attacker can block network for authentic users by flooding or jamming the signal.

2. Spamming

If there are spam messages in VANET then they may elevate the risk of increased transmission latency. As VANET lacks the presence of some basic infrastructure and centralized administration spamming is very difficult to control.

3. Black Hole Attack

If a node drops all the messages coming to it for routing purpose is called as black hole attack or we can say that when a node refused to participate in the network is called as black hole attack.

4.Replay Attack

In replay attack an attacker repeatedly injects data into network to degrade the performance of the network.

5.GPS Spoofing

It is a type of attack in which a malicious driver uses a Global Positioning System (GPS) satellite simulator to generate stronger signals than those generated by genuine satellite. By using this GPS simulator an attack can make fool other drivers that they are in a different location by providing false reading in victim's GPS device.

6.Position Faking

Unsecure communication in VANET can allow an attacker to modify its actual position to another position and pass it to other vehicles. In this way he is broadcasting its fake position which may cause damage to many lives.

7.Message Tampering

It is a threat to authenticity. If an unauthorized user is able to modify the messages exchanged during vehicle-to-vehicle or vehicle-to-infrastructure communication then he/she may inject false information in the network which may cause damage to many lives.

8. Broadcast Tampering

This type of attack is performed by an insider attacker in which an attacker injects false messages in the network to cause damage.

9.Malware

It is a type of attack in which a virus or worm is entered into the VANET and make communication very slow by eating resources. Virus and worms may enter in VANET during software or firmware upgrade in OBU and RSU or an insider attack may manually inject virus or worm in the OBU or RSU.

10. Sybil Attack

It is type of attack in which a malicious driver creates multiple fake identities to make illusion that there is very heavy traffic nearby him so the traffic following him may choose alternate route and attacker would get empty route for himself.

A. SYBIL ATTACK DETECTION APPROACHES

The existing Sybil detection approaches are: The Sybil attack was first described and formalized by Douceur. In a VANET, a node has knowledge about its neighbourhood only with messages it receives. The Sybil attack consists in sending multiple messages from one node (the attacker) with multiple identities. Hence, the attacker simulates several nodes in the network. Different types of attacks that can be launched with Sybil nodes in sensor networks a. Applications of the Sybil attack to Vehicular Ad-Hoc Networks have been discussed. The goal of these attacks could be to give an illusion of a traffic jam to force other vehicles to leave the road to the benefit of the attacker. But the attack could be more dangerous, targeting directly human life for instance, trying to provoke collision in a vehicle platoon .This shows the importance of detecting Sybil nodes in VANET.

One important result shown is that without a logically centralized authority, Sybil attacks are always possible (*i.e.* may remain undetected) except under extreme and unrealistic assumption of resource parity and coordination among entities. That is to say, entities have the same resources constraints, all identities are validated simultaneously by all entities.

Douceur and Newsome and al. proposed resources testing as a defense against Sybil attack.

This resource testing is based on the assumption that each physical entity is limited in some resource. The method described in uses computational puzzles to test nodes computational resources. In, the authors show that this approach is not suitable to ad-hoc networks, and hence typically VANET, because the attacker can have more computational resources than a *honest* node. Moreover, they emphasize a problem of network congestion due to the multiple requests/replies for identities checking. In-stead, they propose a radio resource testing. However, in VANET the attacker can use multiple radio devices to overcome this detection method. Some of the researchers have tried to solve the security problem of the Sybil attack with public key cryptography and authentication mechanism. The authors propose the use of a PKI for VANET (VPKI). They describe a complete solution to provide security of communications and they address the problem of key distribution and privacy. They also propose a mechanism for the most challenging problem: the key revocation. This solution is based on a set of three revocation protocols and a kind of base stations support to send revocation messages. As each vehicle may be authenticated with public key cryptography, the Sybil attack is always detected. Nevertheless, deploying PKI for VANET is a heavy and difficult solution that must be tested to assess its possible use in a real world due to the VANET characteristics. In a VANET, access to network infrastructure is not guaranteed and cryptographic processing may be too long to be usable.

Another possibility to defeat Sybil attack is to provide the security of the positioning system and the reliability of the position claimed by vehicles.

There are also some methods for determining a transmitting peer's node location using signal properties and trusted peers collaboration for identification and authentication purposes. The method uses characteristics such as signal strength and direction so it assumes directional antennas and node's cooperation.

To avoid the deployment of a public key infrastructure within VANET, or the addition of specific devices allowing to detect Sybil nodes, some research works use the received signal power to deduce some inconsistencies between the power of the signal and the claimed position. When a node received a beacon message, it collects signal strength measurement from this node and estimates its new position. A node is considered suspect if its claimed position is too far from the evaluated one.

B. DSDV PROTOCOL

Proactive routing protocol maintains constant and updated routing information for each pair of networking nodes by propagating route updates proactively at fixed interval of time. The periodic and event-driven messages are responsible for route establishment and route maintenance. The Destination-Sequenced Distance Vector (DSDV) protocol is the commonly used proactive routing protocol in vehicle ad hoc network (VANET). In DSDV, each node maintains a routing table with one route entry for each destination in which the shortest path is recorded. It uses a destination sequence number to avoid routing loops. Prior to the establishment of communication between the source and receiver node, the routing protocol should be mentioned to find the route between them. Data Transmission is established between nodes using UDP agent and CBR traffic. Routing process follows DSDV routing protocol.

V. DESIGN OF SYBIL DEFENSE ALGORITHM

Sybil attack detection phases is shown in Figure 1. in this figure malicious node with M, Sybil node with S and The Node that is the identity of his spoofing with A is labelled. In phase1, each vehicle should be registered in a group and receive its public authentication key (AK) before any message transmission. For signing a message, the vehicle uses group authentication key and encryption function and sends it along with original message to other vehicle and RSU. Therefore it is not obligatory for each member to have other members private information such as their identity and public key for authenticating them. Receivers verify a member’s authenticity by signature verification. It’s attained by reconfirmation of encryption function with authentication key to the received message and comparing the result to the signature. Also, receivers can make sure of transmitted data integrity.

In phase2, Because RSU don't have a private key of CAl, so RSU cannot decrypt the message. It is sending a request to CAl to decrypted of the OBUID, in this phase decrypted only IDA.

In phase3, because CAl don't have private key of vehicle A, so CAl cannot decrypted HSK(IDA|HAK(M)) , therefore send a request private key of vehicle A to the CAh.

In phase4, CAh reply private key of vehicle A to CAl and CAl attained by reconfirmation of encryption function with key of vehicle A to the (IDA|HAK(M)) and comparing the result to the HSK(IDA|HAK(M)). Also, CAl can detect the Sybil attack , if result of this comparison is different.

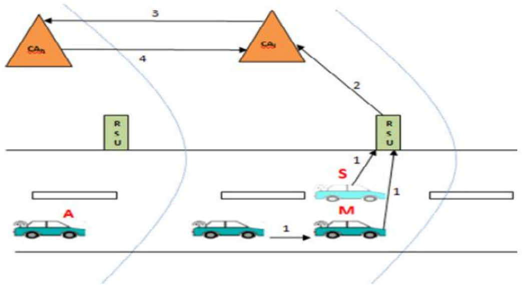

Figure 3. Phases of sybil attack detection

```
Algorithm used for Sybil attack detection
1- EH(PUAK(M)) from source node S
2- EH(SKA(IDA| HAK(M))) from source node S
3- E(PUCA(IDA, HSKA(IDA| HAK(M)))) from node S
4- SEND(RQST(M,HAK(M),CAh,OBUId) from source node S to local RSU other
   vehicle in local region)
5- EH(PUAK(M)) in RSU and IF(HAK(M)==HAK(M)) THEN go to step 7 else go to step 6
6- REPORT to CAl "the message is fault"
7- D(SKCl(IDA, HSKA(IdA| HAK(M))) in CAl
8- REQST(PUA) to CAh
9- RPLY(PUA) to CAl
10-EH(SKA(IDA|HAK(M)))and IF(HSKA(IDA|HAK(M))==HSKA(IDA|HAK(M)))
   THEN Sybil attack detect.
```

Notation Means

RQST Request from source node

RPLY Reply from VANET server

SEND Send key from VANET server to destination

E (…) Encryption of Message

EH(…) Encryption of Message with hashing function

D (…) Decryption of Message

PUA Public key for source node A

SKA Private Key for source node A

M Original message

AK Shared key between all nodes is located in a area

HAK(M) Encryption message with Key AK

CAh Home CA or initial CA

CAl Local CA

IDA Identifier of vehicle

VI. Performance Analysis

In this section, we will evaluate our proposed Sybil attack detection technique agreement scheme from the aspect of efficiency and network performance.

1) Efficiency Analysis: In this part, we evaluate and compare the performance of our protocol with the other protocols, which offer similar security and privacy properties even though different schemes were adopted, The experimentation results of the crypto overhead are listed in Table 1.We compare our protocol with several existing CL-AKA protocols we have referred above in Table 2. As shown in Figure 3, Figure 4 and Figure 5, we can see that our scheme has obvious advantages in computational efficiency after multi-times key agreement.

2) Network Performance: we use the most widely accepted ones: the packet delivery ratio (PDR), end-to end delay (E2ED).

The results are shown in Figure 6, Figure 7. In both figures, the x-axis indicates the mean speed of the 200 vehicles in the scenario. In Figure 7, the y-axis indicates the package delivery rate, which means the ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

$$PDR = \frac{\sum Numberofpacketreceive}{\sum Numberofpacketsend} \quad (7)$$

Table 1. Crypto Overhead

Operations	From	Naive (time(ms))	Comba (time(ms))
PointMultiplicationE_1	xP	1.8444	0.4124
Modular Exponentiation E2	g^x mod n	3.2028	0.7070
Multiplication M	ab mod n	0.0334	
Map-to-PointHash Function H	H:{0,1}*G	0.9180	

Table 2. Comparison of Different Protocol

Operations	From	Naive (time(ms))	Comba (time(ms))
Huang	$3E_1 + 2e$	50.8125	46.5192
Lippold	$5E_1$+10e+ 2H	237.468	230.308
Song	$16E_2 + 4M$	51.3784	11.4456
Yang	$9E_2 + 3M$	28.9254	6.4632
	$9E_2 + 2M$	28.8920	6.4298
Proposed			

From Figure 6, we can see that the three curves are very similar, and they are nearly overlapped. Therefore, the proposed scheme does not decrease the packet delivery rate and does not add much network overhead.

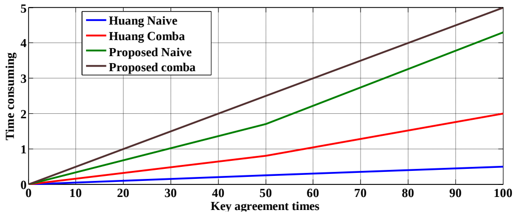

Figure 3. Compared with Huang's schemes

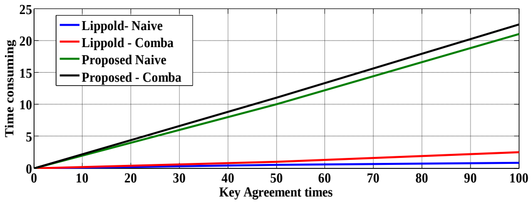

Figure 4. Compared with Lippold's schemes

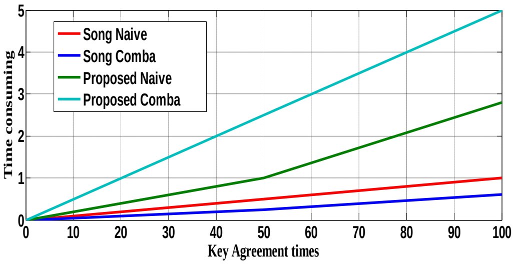

Figure 5. Compared with Song and Proposed scheme

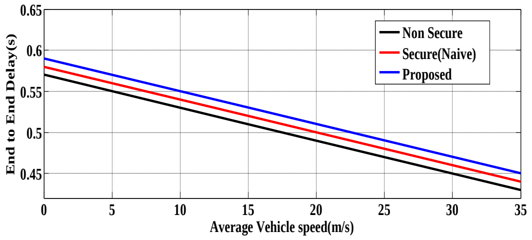

Figure 6. Packet delivery rate results

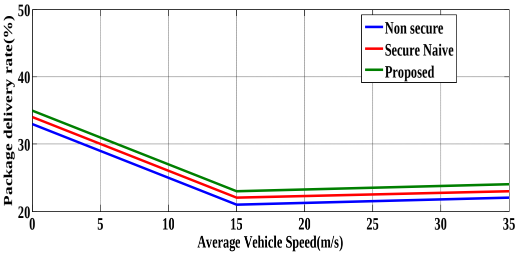

Figure 7. End-to-end delay results

In Figure 7, the y-axis indicates the end-to-end delay, E2ED means the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only these data packets are successfully delivered to destinations count.

$$E2ED = \frac{\sum arrivetime - sendtime}{\sum Numberofconnections} \qquad (8)$$

From Figure 7, we can see that the proposed scheme increases a little extra end-to-end delay, but the addition in E2ED is negligible because the three curves is quite close. We can conclude that our proposed Sybil attack detection scheme is efficient which shows a good network performance.

VII. Conclusion

In this paper, we have developed a Sybil attack detection scheme for urban vehicular networks on DSDV protocol. Consecutive authorized messages obtained by an anonymous vehicle from RSUs form a trajectory to identify the corresponding vehicle. Location privacy of vehicles is preserved by realizing a location-hidden signature scheme. Utilizing social relationship among trajectories, The detection technique can find and eliminate Sybil trajectories. The detection technique design can be incrementally implemented in a large city. It is also demonstrated by both analysis and extensive trace driven simulations that Sybil detection technique can largely restrict Sybil attacks and can enormously reduce the impact of Sybil attacks in urban settings.

First, in Sybil detection technique, we assume that all RSUs are trustworthy. However, if an RSU is compromised, it can help a malicious vehicle generate fake legal trajectories. In that case, Sybil detection technique cannot detect such trajectories. However, the corrupted RSU cannot deny a link tag generated by itself nor forge link tags generated by other RSUs, which can be utilized to detect a compromised RSU in the system. In future work, we will consider if RSU is not available how to do node identity verification and detect Sybil attacks. We will also develop cost-efficient techniques to fast detect the corruption of an RSU.

REFERENCES

[1]. Jun, S., Chunjiao, HE., Lei, Z., Shanyu, T., and Huango, Z., "Toward an RSU – unavailable Lightweight Certificateless Key Agreement Scheme for VANETs", *China Communications*, 11, 9, September 2014, pp. 93-103.

[2]. Lu, R., Lin, X., Zhu, H., Ho, PH., and Shen, X., "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications", *IEEE INFOCOM 2008 proceedings*, 2008, pp. 1903-1911.

[3]. Sharif, BS., Blythe., PT., Almajnooni, SM. and Tsimenidis, CC., "Inter-vehicle mobile ad hoc network for road transport systems', *IET Intelligent Transport Systems*, 1, 1, January 2007, pp. 47-56.

[4]. Song, J., Zhuang, Y., Pan, J., and Cai, L., "Certificateless secure upload for drive-thru internet", *IEEE International Conference on Communications*, 60, 2, 2011, pp. 580-591.

[5]. Lippold, G., Boyd, C., and Nieto, JG., 'Strongly secure certificateless key agreement', *Springer Berlin Heidelberg Palo Alto, CA, USA*, 2009, pp. 206-330.

[6]. [6] H. Yu, M. Kaminsky, P.B. Gibbons, and A. Flaxman, "Sybilguard:Defending against Sybil Attacks via Social Networks," *Proc.SIGCOMM*, Sept. 2006, pp. 267-278.

[7]. M.S. Bouassida, G. Guette, M. Shawky, and B. Ducourthial, "Sybil Nodes Detection Based on Received Signal Strength Variations within Vanet," *Int'l J. Network Security*, vol. 9, no. 1, 2009, pp. 22-32.

[8]. Yang, G., and Tan CH., " Strongly secure Certificateless key without pairing", *Proceedings of the 4th international symposium on information, Computer and Communications Security, ACM,* 2011, pp. 71-79.

[9]. Dent, AW., "A survey of certificateless encryption schemes and security models", *International Journal of Information Security,* 7, 5, 2008, pp. 349-377.

[10]. B. Xiao, B. Yu, and C. Gao, "Detection and Localization of Sybil Nodes in Vanets," Proc. Workshop Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks (DIWANS '06), Sept. 2006, pp. 1-8

[11]. Shamir, A., "Identity – based cryptosystems, and signature schemes", 196, 2000, pp. 47-53.

[12]. T. Zhou, R.R. Choudhury, P. Ning, and K. Chakrabarty, "Privacy-Preserving Detection of Sybil Attacks in Vehicular Ad Hoc Networks," Proc. Fourth Ann. Int'l Conf. Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous '07), Aug.2007, pp. 1-8.

[13]. Boneh, D., Lynn, B., and Shacham, H.," Short Signatures from the Weil Paring", *Springer Berlin Heidelberg*, 2001, pp. 514-532.

[14]. Dong, X., Wei, L., Zhu, H., Cao, Z., and Wang, L., "An Efficient Privacy Preserving Data Forwarding Scheme for Service-Oriented vehicular Ad-hoc networks", *IEEE Transactions on vehicular technology*, 60, 2, 2011, pp. 580-591.

[15]. Xiong, H., Beznosov, K., Qin, Z., and Ripeanu, M., " Efficient and Spontaneous Privacy-Preserving Protocol for Secure Vehicular Communication", *IEEE ICC 2010 proceedings*, 2010.

[16]. Kushwaha, D, Shukla, P K and Baraskar, R., "A Survey on Sybil Attack in Vehicular Ad-hoc Network", International Journal of Computer Applications, vol. 98, no. 15, pp. 31-36.