International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

Decentralized Sybil Attack Prevention in VANET using Elliptic Curve Cryptography.

Suhaib Rehman, Nitika Kapoor

Abstract: ***The existence of vehicular ad-hoc network (VANET) depends on secure message dissemination. Among the various possible attacks on VANET, sybil attack is the root cause of other attacks and it can violate the fundamental assumption of VANET. Our proposal helps in preventing Sybil attack during the initial phase of authentication by proposing three level network model. On the top is Cloud-based Trusted Authority (CTA) which maintains database of all the valid vehicles (global database) and generates Elliptic Curve domain parameters. In the middle is the RSU-Manager (RSU_M) level which maintains the database of local vehicles of a particular area and at the bottom are the RSUs and vehicles. Elliptic Curve Cryptography is used as the cryptographic algorithm during message dissemination with the aim of increasing performance and security. The comparison of hash of vehicle information is performed for authentication of vehicle during vehicle to infrastructure interaction. Authentication of Vehicle in first phase is performed at RSU_M and in second phase at the CTA, in case the vehicle information is not found in the database of RSU_M. Our proposed model provides flexibility, lower latency and reduces network overhead. This paper demonstrates the proposed scheme for detecting sybil node in an effective manner.***

Index Terms: ***Cloud-based Trusted Authority (CTA), Elliptic Curve Digital Signature Algorithm (ECDSA), Roadside Unit-Manager, Sybil Attack, Transport Authority, Vehicular Ad-hoc Network (VANET)***

I. INTRODUCTION

In the recent years the development of technology in cars has considerably increased. Modern cars are equipped with various electronic components called On-Board units(OBUs) which are responsible for communicating with OBU's of other vehicles and with the Road Side Units(RSU's) .So, VANET is the special case of MANET where exchange of safety and non-safety messages takes place between Vehicle to Vehicle (V2V) or Vehicle to Infrastructure(V2I).Figure 1 shows the architecture of VANET. In VANET messages should exchange securely among Vehicles or with the infrastructure and no attacker should be able to delete or modify them [11]. So, like traditional network, VANET has also security concerns comprises of availability, integrity, confidentially, authentication and non-repudiations. Different types of attacks are possible on VANET but sybil attack introduced in [5] is one the most harmful attacks as it the root cause of other possible attacks. In sybil attack, an attacker can generate multiple virtual fake identities/node called sybil nodes to impersonate normal nodes in the VANET [15]. Sybil attack is responsible for violating the fundamental assumptions of VANET [10] In sybil attack , attacker can create virtual fake identities with false location making the illusion of heavy traffic for other nearby vehicles by which forcing the normal nearby vehicles to take different routes and attacker can get the road with less or no traffic[16].As sybil attack is the root cause of other attacks, it can also bombard vehicles or infrastructure with heavy traffic which results in choking the bandwidth and hence degrading overall performance of the network. Sybil nodes are also responsible for black hole attack in which sybil nodes could drop all the messages go through them in multipath routing [8]

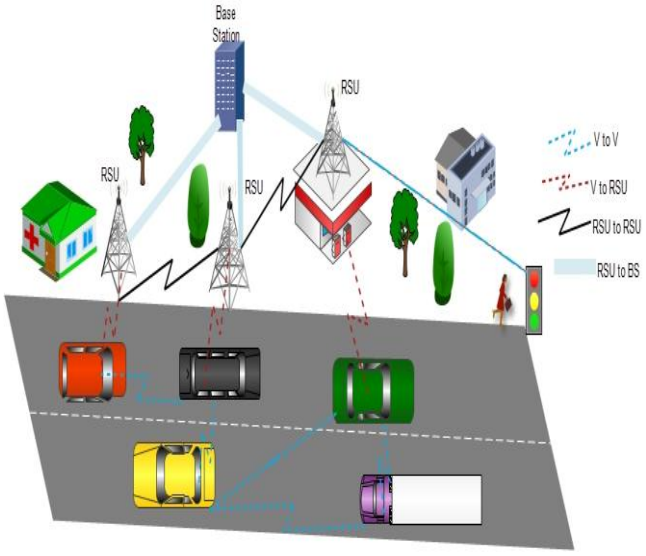

Figure 1. Architecture of VANET

All the techniques proposed by different researchers for sybil attack detection are classified into three broad categories: 1) Resource-based testing methods. 2) Position verification-based methods. 3) Trusted certification-based methods. The resource testing-based approach has the assumption that each physical node in VANET have limited computation and communication resources. This type of technique may become invalid if the attacker node has more computation and communication resources to carry out sybil attack. Trusted certification-based approach uses digital signatures, certificate authority, cryptographic algorithms, public key infrastructures (PKI). These methods help in finding node at the beginning of the attack. But due to dynamic topology of VANETs most of these methods having centralized authority for digital signatures and certification distribution are not suitable.

Revised Manuscript Received on 30 May 2019.
***** Correspondence Author
Suhaib Rehman*, Department of Computer Science & Engineering, Chandigarh University, Mohali, Punjab, India
Nitika Kapoor, Department of Computer Science & Engineering, Chandigarh University, Mohali, Punjab, India

Position verification-based approach measures the physical quantities. The physical quantities used to detect the sybil attack include Received Signal Strength (RSSI), Angle of Arrival (AoA), Time Difference of Arrival (TDoA). Although position verification based methods are light weight as compared to trusted certification based methods but it has some major issues like in RSSI-based sybil attack detection, the estimation accuracy heavily depends on the propagation model assumed .RSSI-based methods are also not able to detect malicious node that have ability to manipulate the transmission power and this heavily depend on the honesty and trustworthiness of neighboring nodes. Some RSSI-based methods use trusted centralized station for sybil attack detections. Also, deployment of such infrastructure is quite difficult at the initial stage of VANETs [**Error! Reference source not found.**].

Among the various asymmetric cryptographic algorithms, Elliptic Curve Cryptography (ECC) provides better security for a given key size. In paper[**Error! Reference source not found.**]160bits of key size in ECC provide same level of security as 1024 bits of key size in RSA. Hence ECC provides better performance, less complexity. Also, smaller keys mean less heat and power consumption [**Error! Reference source not found.**]

Akeel et al. [**Error! Reference source not found.**]have provided mathematical overview of Elliptical Curve Digital Signature Algorithm (ECDSA) and have compared ECC key size with RSA and DSA .

Teniou et al. [**Error! Reference source not found.**] have proposed distributed scheme for certificate generation called as Elliptic Curve Qu-Vanstone (ECQV). The concept of Cloud Certificate Authority and RSU-Managers are also introduced for flexibility and less latency.

In this paper, we propose a light weight approach for preventing sybil attack in a decentralized network model using Elliptic Curve Cryptography (ECC) as authentication scheme to overcome the security concerns like node authentication, message authentication, privacy and reduce network overhead. Sybil node is detected at different levels of our network model and hence reduce latency and overall burden on single entity.

II. RELATED WORK

Sybil attack was first coined by Douceur [**Error! Reference source not found.**] in distributed computing environment. In the absence of identification authority, a node is probably a sybil node if it can't solve the random puzzle within limited time frame by taking into consideration that each node has limited resources, but this approach becomes invalid if node has enough resources.

Chen et al.[**Error! Reference source not found.**] have proposed a scheme to detect sybil attack by comparing the difference of digital certificates vectors of neighboring nodes. This method is suitable at initial stages of VANET.

Chen et al.[**Error! Reference source not found.**] have introduced Difference of two (DOT), which calculate difference of Radio Signal Strength (RSS) between landmarks that have different transmission levels to detect identity-based attack in wireless and sensor networks.

Zhou et al. [**Error! Reference source not found.**] have proposed a protocol called as Privacy Preserving Detection of Abuses of Pseudonyms" (P2DAP). They assumed Department of motor vehicle (DVM) manages and maintains pseudonyms for all vehicles. Multiple pseudonyms are generated for one vehicle with hash. A trusted vehicle sends one event with one pseudonym and if RSU detects one event is signed by multiple pseudonyms with same hash it marks it as malicious and send it to DVM for further action.

Mekliche et al. [**Error! Reference source not found.**] improved P2PDAP known as L-P2DSA. In this proposed method the burden on DVM is reduced by involving it only when sybil node is detected. Second screening is done at RSU level to reduce number of false alarms. RSS and AoA is used to find the location of suspicious vehicles and are detected as sybil nodes if they are verified at similar locations.

Chang et al. [**Error! Reference source not found.**] proposed a scheme named footprint to detect sybil attack using trajectories of vehicles. An authorized message is sent by RSU for each vehicle as the Proof of Presence (PoP) at this RSU. The location of vehicles is preserved by keeping RSU anonymous while signing messages (signer-ambiguous). Also authorised messages are recognizable if they are issued by same RSU at the same time i.e. they are temporarily linkable. Trajectories of vehicles using subgraphs of undirected graph are used to detected sybil nodes as the probability of two nodes having same trajectories is very low. The drawback of this approach is that all vehicles need to know the whole infrastructure layout of RSUs. Also comparing the trajectories pairwise is quite complex.

Shrestha et al [**Error! Reference source not found.**] have used RSS to differentiate between benign nodes from sybil node without calculating the location of sybil nodes. After collecting the large samples from each node in the VANET and distance between two different signal vectors is compared with threshold value to determine whether the node is legitimate node or a sybil node.

Alimohammadi et al. [**Error! Reference source not found.**] have proposed a protocol based on short group signature scheme. RSU is responsible for verification of vehicle in first phase and after successful authentication a group private key is allotted to the vehicle which is used to communicate with other valid vehicles in the network. All sybil nodes are detected non-central without the involvement of RSUs.

Reddy et al. [**Error! Reference source not found.**] have proposed cryptographic digital signature (DS) system to develop thrust among the communicating entities. VANET Server stores vehicle ID and Master Key and then forwards the unique vehicle ID to the Local VANET Server which after confirmation generates Local Certificate, Session Key and RSU number for the purpose of detecting sybil attack.

Yao et al. [**Error! Reference source not found.**]. have used Received Signal Strength Indicator (RSS) time series called Voiceprint (vehicular speech) for detecting malicious nodes without relying on other vehicles in the network.

Sybil nodes are detecting based on similar pattern in RSSI time series.

Yao et al. [**Error! Reference source not found.**] have improved the Voiceprint method by detecting sybil attack on SCH using power control and reducing observation and false positive rate.

III. PROPOSED NETWORK MODEL

Our proposed model is divided into three levels. On the top level is Cloud-based Trusted Authority (CTA), in the middle level are RSU-Managers (RSU_{Ms}), and on the bottom level are RSUs and Vehicles. There is also a Transport Authority (TA) which helps in uploading vehicle information on CTA and to the vehicle. Figure 2 represents the proposed network model. 1) Cloud-based Trusted Authority (CTA): CTA is placed on the top of our network model. CTA is responsible for storing and maintaining the information of all vehicles (V_{info}) in its global database in a secure way uploaded by Transport Authority (TA). It is responsible for generating Elliptic Curve (EC) domain parameters: q, a, b, G, n, h in a finite field [ECC].

Here,

q	Field size.
a and b	Coefficients of EC.
G	Generator.
n	Order of G..
h	Cofactor ∃ *nh* are pts. on EC.

It not only manages RSU_M placed under it but also updates the local database of RSU_M in case the information of vehicle is not found at RSU_M level during authentication process.

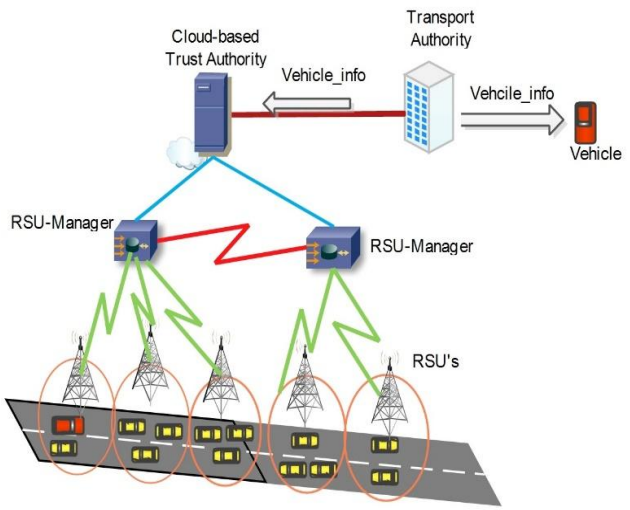

Figure 2. Proposed Network Model

2) RSU-Managers (RSU_M): RSU_M are placed in the middle level of network model. Each RSU_M is responsible for managing the RSUs according to the geographical area depict in figure 2. RSU_M not only manages the RSUs of that area but also stores the frequently travelling vehicle information in its secure local database. i.e. local database which is the subset of global database stored at CTA. RSU_M is also responsible for requesting V_{info} of vehicle in case it is not found in the database of RSU_M. Maintaining local database at RSU_M has two reasons: a) It reduces the exchanges of messages to CTA and hence provides decentralized model for sybil attack detection. b) The probability of vehicle to travel along same trajectory on daily basis is maximum. E.g. The local vehicle of area Chandigarh (one of the states of India) has maximum probability of travelling in or near the same area, maintaining the local database reduces the distance to travel the data packets to verify the vehicle and hence reduces the latency and overall burden on the network particularly on CTA.

3) Road Side Units (RSUs) and Vehicles: RSUs are densely deployed devices on the road side. They are responsible for broadcasting information about neighboring vehicles, weather, road condition, provides internet facility etc. to the vehicles. RSUs in our proposed scheme also maintains a list of the malicious nodes to detect if same malicious vehicle frequently tries to gain access into the network during the initial phase of authentication. They also to and fro messages between vehicles and RSU_M. Each vehicle is equipped with necessary sensors, OBUs and also have tampered proof device used to store critical vehicle information.

A. Assumptions:

In our proposed scheme following assumptions are taken into consideration:

1). Vehicles are equipped with tampered proof device used to store critical vehicle information.

2). TA is trusted organization responsible for storing data on Cloud-base Trusted Authority and onto the vehicle in a secure way.

3). Any kind of minacious among TA, CTA, RSU_M and RSUs has not been considered

4). The grouping of RSUs under RSU_M is pre-defined.

5). The order of performance, storage and bandwidth is as: CTA > RSU_M > RSU > Vehicle.

6). Any kind of message passing scheme or certificate generation procedure after vehicle is authenticated has not been considered.

B. Working of proposed scheme:

Different Authorities in VANET play a vital role for maintaining transparency, monitoring and trust development into the network. One such trusted authority is Transport Authority. In our proposed Scheme TA is used only to store Vehicle information in the database of CTA and Vehicle in a secure way. As TA is not taking active part in detecting sybil node hence in the following sections its way of communication has not been taken into consideration.

1*) Initialization Phase:*

In our proposed scheme, TA during the time of registration stores the Vehicles critical data including vehicle ID (VID) and the Hash (H_N) of Plate number (P_N), Chassis number (C_N), License number (L_N) using SHA-3 on CTA in a secure way. Excluding Hash, all other information (VID, PN, CN, LN) is also stored in tamper proof device of vehicle. Figure 2 depicts the scenario.

$H_N \leftarrow H(P_N, C_N, L_N)$.

$CTA \leftarrow (VID \parallel H_N)$ && $V \leftarrow (VID, P_N, C_N, L_N)$.

CTA decides type of EC by deciding the its domain parameters: q, a, b, G, n, h. A private key P_R(CTA) and public key P_U(CTA) is generated, the domain parameters and P_U(CTA) are available

to public. All other network devices use these parameters to generate their private and public keys

2). *Sybil node detection Phase:*

The working of different entities of our proposed system in detecting sybil node is as:

a) Vehicle to RSU.

Besides EC domain parameters and other information, RSU also periodically announces its

Notation	*Explanation*	Notation	*Explanation*
VID	*Unique vehicle identity*	$P_U(x)$	*Public Key of x*
P_N	*Plate Number*	$P_R(x)$	*Private key of x*
C_N	*Chasses Number*	TA	*Transport Authority*
L_N	*License Number*	RSU	*Road Side Unit*
H_N	*Hash generated by Transport Authority*	RSU_M	*RSU Manager*
H'	*Hash generated by Vehicle*	CTA	*Cloud-base Trusted Authority*
L_M	*List of malicious Vehicles*	ST_V	*Status of the Vehicle*
V_{info}	*Vehicle information*	$Cert_V$	*Certificate of Vehicle*
Note: X is replaced by V, RSU, RSU_M and CTA			

Table 1 Notations

Public key P_U(RSU). When the vehicle come under the vicinity of RSU, Vehicle V, generates the hash of P_N, C_N, L_N at time T and uses its private key and public key of RSU to encrypt the information and send it to the RSU.

$$H' \leftarrow H(P_N, C_N, L_N)$$
$$RSU \leftarrow Vehicle:$$
$$RSU \leftarrow P_U(RSU)[P_R(V) \| VID \| H']$$

Figure 3 shows the direction of message flow of our proposed model.

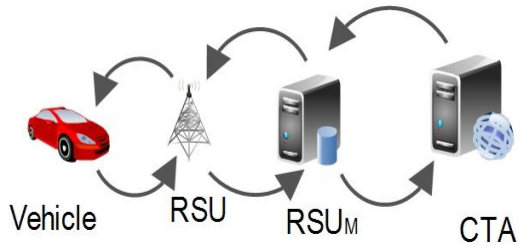

Figure 3. Direction of Message Flow

b) RSU to RSU_M:

After RSU verifies the integrity and authentication of message send by the vehicle, RSU checks in its database whether the vehicle exists in list of malicious vehicles (L_M) or not. If the vehicle entry is in the list, it is discarded for further communication otherwise RSU adds its own Unique identification (RID) to the message and encrypt the message with P_R(RSU) and then with $P_U(RSU_M)$ and sends it to the RSU_M.

$$RSU_M \leftarrow RSU:$$
$$RSU_M \leftarrow P_U(RSU_M)[P_R(RSU) \| VID \| H' \| RID].$$

c) At RSU_M level:

As stated before, RSU_M maintains the local database for the verification of vehicle. The different cases arise at this stage for the verification of the vehicle are as under:

Case 1: When H_N=H';

If after time T+Δt at RSU_M, the hash H_N , of the vehicle already stored by TA on CTA which is further stored on RSU_M by CTA is equal to the hash H' generated by vehicle at time T , then RSU_M request the CTA for the verification of status of vehicle (ST_V) and then generates the certificate ($Cert_V$) for the vehicle which acts as a network key for further communication in the network.

$$CTA \leftarrow RSU_M:$$
$$CTA \leftarrow PU(CTA)[PR(RSU_M) \| VID \| H' \| RID \| RMID]$$

Here, Status of the Vehicle is maintained by CTA determines whether the vehicle is already allotted into the network or not. This ST_V adds one more security level to our network. If somehow the tampered proof device of vehicle is compromised, and the details of vehicle are theft by the attacker. In that case a sybil node may try to use those parameters to generate the same hash but his attempt can be tackled by ST_V, which verifies that same kind of vehicle is already allotted to the network and detect it as sybil node and hence avoid the generation of similar fake identities into the network. If the ST_V signifies that the same type of vehicle is already present into the network, then this Vehicle is declared as Sybil vehicle and L_M is update otherwise if ST_V signifies status of vehicle to be NULL(Here NULL signifies that no such vehicle is allotted to the network), then certificate is generated by CTA and is send to vehicle.

If, ST_V==NULL,

$$RSU_M \leftarrow CTA:$$
$$RSU_M \leftarrow P_U(RSUM)[P_R(CTA) \| VID \| RID \| RIMD \| Cert_V]$$

$$RSU \leftarrow RSU_M:$$
$$RSU \leftarrow P_U(RSU)\,[P_R(RSUM) \| VID \| RID \| Cert_V]$$

$$Vehicle \leftarrow RSU:$$
$$V \leftarrow P_U(V)[P_R(RSU) \| VID \| Cert_V]$$

If, $ST_V \neq$NULL,

Then CTA announces it as sybil node and requests the RSU to update its list of malicious vehicles L_M.

Case 2: When $H_N \neq H'$;

If after time T+Δt, the hash H' generated by the vehicle and the hash H_N already stored by TA are not equal with the corresponding Vehicle ID then the Vehicle is declared as sybil node and L_M maintained at RSU level is updated

Case 3: When V_{info} is not found at RSU_M;

RSU_M has the high probability of storing the information of vehicle frequently visiting that area. There is also frequent possibility that vehicles can come under the control of

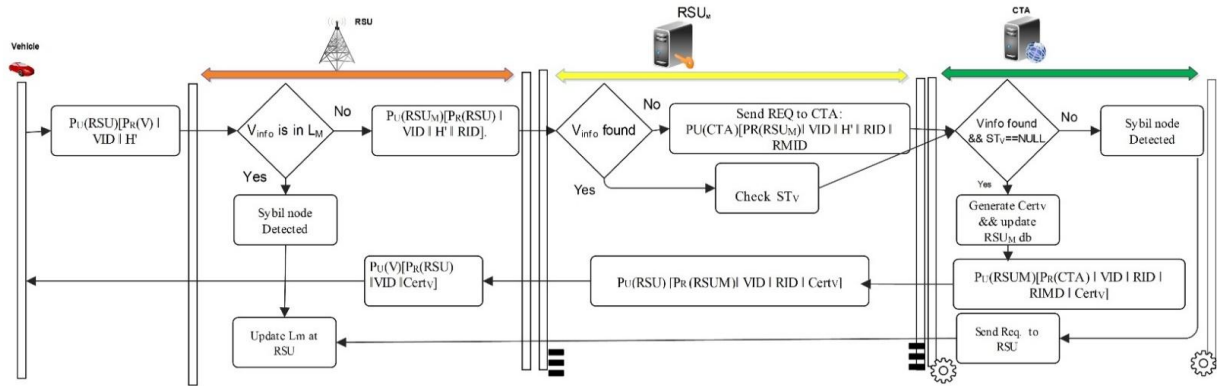

Figure 4. Messages exchanged among Vehicles, RSU, RSU_M and CTA

other RSU_M, in that case RSU_M requests the information about the vehicle from CTA. CTA having the information stored of the vehicles after authentication generates the certificate for the vehicle and also updates the database of RSU_M. In case if the information of vehicle is also not found at CTA then the vehicle is declared as Sybil vehicle and list of malicious vehicles L_M, maintained at RSU level is updated.

Case 3: When V_{info} is not found at RSU_M;

RSU_M has the high probability of storing the information of vehicle frequently visiting that area. There is also frequent possibility that vehicles can come under the control of other RSU_M, in that case RSU_M requests the information about the vehicle from CTA. CTA having the information stored of the vehicles after authentication generates the certificate for the vehicle and also updates the database of RSU_M. In case if the information of vehicle is also not found at CTA then the vehicle is declared as Sybil vehicle and list of malicious vehicles L_M, maintained at RSU level is updated.

Figure 4 gives the overall view of messages exchange among different entities of our proposed system.

ALGORITHM

Step 1: Repeat for each vehicle V (VID, P_N, C_N, L_N)

a) Initialization

At TA,

$H_N \leftarrow H(P_N, C_N, L_N)$ *// TA generates hash*

$CTA \leftarrow H_N \| VID$ *// TA stores hash and VID on CTA*

$V \leftarrow (VID, P_N, C_N, L_N)$ *// stores Vinfo on db of vehicle*

At V,

$H' \leftarrow H(P_N, C_N, L_N)$ *// generates hash*

$V \leftarrow H'$ *// stores hash on the vehicle*

b) Authentication

Step 2: At RSU,

if V_{info} is in L_M *// Malicious/sybil node detected*

goto **Step 7**.

else forward V_{info} to RSU_M

goto **Step 3**.

Step 3: At RSU_M,

if V_{info} not found

forward V_{info} to CTA

goto **Step 4**.

else

goto **Step 6.**

Step 4: At CTA,

if V_{info} not found *//sybil node*

goto **Step 7**

else

goto **Step 5**

Step 5: At CTA Check ST_V,

if ST_V=NULL *// STv signifies vehicle is already not present.*

vehicle is valid, generate ($Cert_V$)

else

goto **Step 7**

Step 6: if $H' \neq H_N$ *// Sybil node.*

goto **Step 7**

else

$H' == H_N$

goto **Step 5**

Step 7: Vehicle is sybil Vehicle

update (L_M).

IV. PERFORMANCE EVALUATION

Our proposed scheme is simulated on omnet-4.6 simulation tool integrated with inetmanet-2.0 and sumo-0.21.

The specification of computer on which the proposed network is simulated are:

Processor	I5, 2.5GHZ
RAM	8GB
OS	Windows OS, Version-10

A) *Simulation setup:*

A two-way road having 200 vehicles with average speed of each vehicle set to 40km/h and communication range of 300m.AODV protocol is used for routing because of its reactive nature, so it maintains route discovery only when there is demand of sending data and hence considerably decrease the memory consumption. It can therefore be used in large network. More ever our proposed scheme of sybil attack detection is independent on selection of routing protocol.

Table 2 shows the simulation parameter considered

B) *Performance Analysis:*

Our simulation setup verifies the performance of detecting sybil node based on parameters: delay, throughput and packet delivery ratio w.r.t the number of vehicles

1) Delay: The latency for authentication of node depends on the time a packet takes from its generation from sender to the successfully received by the receiver. Delay in sending single packet is

Delay= n(ttrans + tq + tcont + tproc + tprop + tgen + tver)

Here,

n	No. of hops b/w source and destination.
ttrans	Transmission delay.
tq	Queuing delay.
tcont	Contention delay
tproc	Processing delay.
tprop	Propagation delay
tgen	Hash generation delay.
tver	Hash verification delay.

The parameters mentioned above for total delay is already considered in simulation. Figure 5(a) shows the relation of delay with the number of vehicles present in the network. This graph shows if the number of vehicles increase the increase in delay is very less.

Table 2 Simulation parameters

Parameters	Value
Area	2500m X 2500m
Total number of vehicles	200
Average speed of vehicles	40km/h
Total number of RSUs	4
Total number of RSU-Managers	2
Number of Cloud-based Trust Authority	1
Bandwidth	2Mbps
Simulation time	500s
Protocol	AODV

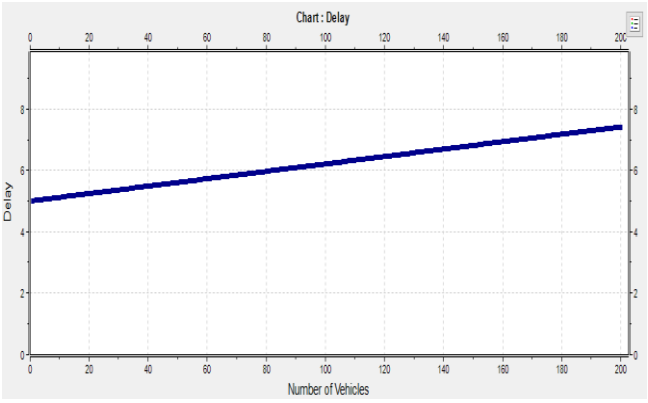

Figure 5(a). Delay vs Number of Vehicles

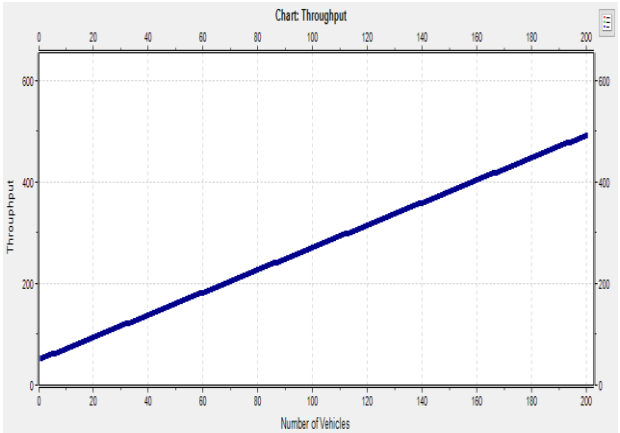

Figure 5(b). Throughput vs Number of Vehicles

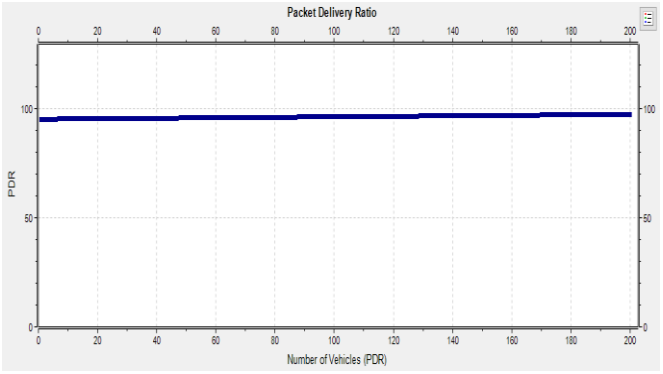

Figure 5(c). PDR vs Number of Vehicles

2) Throughput: It is defined as the rate at which packet are successfully send over the channel to the destination and is measured in bit per second.

$$Throughput = \frac{\sum_{a=1}^{n} recv}{PkTduration}$$

3) Packet Delivery Ratio (PDR): PDR is the total packet received with respect to the total packet send. If "R" represents the total packets received and "S" represents total packet send, then;

$$PDF = \frac{R}{S} \text{ x } 100.$$

Figure 5(b) and Figure 5(c) shows the dependency of Throughput and PDR on the number of vehicles.

As stated above in section III, we are following decentralized approach for sybil attack detection, which not only reduces the overload on single network device but also decrease search time and latency. Implementing ECC improves performance and security as compared to other cryptographic algorithms like DES, AES, RSA etc. Figure 6 shows the transfer of packet during V2V and V2I communication. For better visualization we have randomly taken few vehicles out of 200 Vehicles.

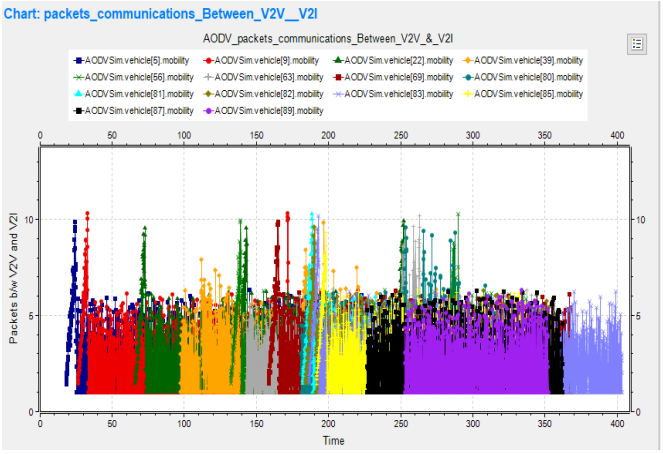

Figure 5. Packet transfer between V2V and V2I

In our simulation we have intentionally inserted 5% of malicious node into network as shown in Figure 6, red dotted vehicles represent sybil node and green dotted vehicles shows trusted vehicles. The average PDR is ≈ 97%

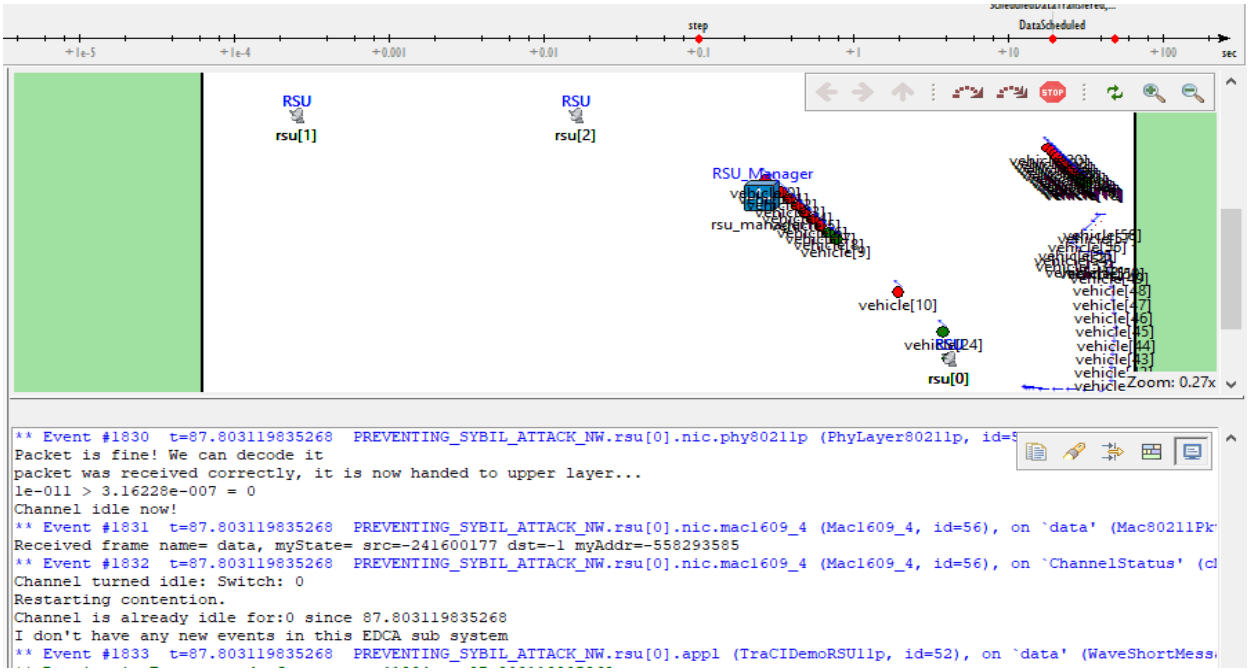

Figure 6. Simulation Window

indicating an efficient behavior in node authentication and sybil node detection in our proposed system.

V. CONCLUSION

We have proposed a lightweight and efficient protocol for authenticating and detecting sybil nodes in a decentralized manner. The validity of node is first verified by the RSU using list of malicious vehicles. After passing this stage, request is forwarded to the RSU_M which has the information of all the local vehicles of that area. If the vehicle information is not found at RSU_M, it forwards request to the CTA which not only verifies vehicle information but also checks the status of all vehicles. Checking status of vehicles eliminates the chance of having replica of the vehicle. The proposed multistage authentication scheme not only reduces latency but also decrease the time to search vehicle information during the authentication process. Using ECC increases performance, reduces power, storage consumption and complexity of the network. It also decreases the overall size of data packet by decreasing key size without compromising with the security of the network.

REFERENCES

1. Mahdiyeh Alimohammadi and Ali A Pouyan. Sybil attack detection using a low cost short group signature in vanet. In *2015 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, pages 23–28. IEEE, 2015.
2. Shan Chang, Yong Qi, Hongzi Zhu, Jizhong Zhao, and Xuemin Shen. Footprint: detecting sybil attacks in urban vehicular networks. *IEEE Transactions on Parallel and Distributed Systems*, 23(6):1103–1114, 2012.
3. Chen Chen, Xin Wang, Weili Han, and Binyu Zang. A robust detection of the sybil attack in urban vanets. In *2009 29th IEEE International Conference on Distributed Computing Systems Workshops*, pages 270–276. IEEE, 2009.
4. Yingying Chen, Jie Yang, Wade Trappe, and Richard P Martin. Detecting and localizing identity-based attacks in wireless and sensor networks. *IEEE Transactions on Vehicular Technology*, 59(5):2418–2434, 2010.
5. John R Douceur. The sybil attack. In *International workshop on peer-to-peer systems*, pages 251–260. Springer, 2002.
6. P Gallagher. Federal information processing standards publication digital signature standard (dss). *Fips pub 186-3*, 2009.
7. Aqeel Khalique, Kuldip Singh, and Sandeep Sood. Implementation of elliptic curve digital signature algorithm. *International journal of computer applications*, 2(2):21–27, 2010.
8. Mohamed Nidhal Mejri, Jalel Ben-Othman, and Mohamed Hamdi. Survey on vanet security challenges and possible cryptographic solutions. *Vehicular Communications*, 1(2):53–66, 2014.
9. Kenza Mekliche and Samira Moussaoui. L-p2dsa: Location-based privacy-preserving detection of sybil attacks. In *2013 11th International Symposium on Programming and Systems (ISPS)*, pages 187–192. IEEE, 2013..
10. Soyoung Park, Baber Aslam, Damla Turgut, and Cliff C Zou. Defense against sybil attack in vehicular ad hoc network based on roadside unit support. In *MILCOM 2009-2009 IEEE Military Communications Conference*, pages 1–7. IEEE, 2009.
11. Maxim Raya and Jean-Pierre Hubaux. Securing vehicular ad hoc networks. *Journal of computer security*, 15(1):39–68, 2007.
12. D Srinivas Reddy, V Bapuji, A Govardhan, and SSVN Sarma. Sybil attack detection technique using session key certificate in vehicular ad hoc networks. In *2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)*, pages 1–5. IEEE, 2017.
13. Rakesh Shrestha, Sirojiddin Djuraev, and Seung Yeob Nam. Sybil attack detection in vehicular network based on received signal strength. In *2014 International Conference on Connected Vehicles and Expo (ICCVE)*, pages 745–746. IEEE, 2014.
14. Ahcene Teniou and Boucif A Bensaber. Efficient and dynamic elliptic curve qu-vanstone implicit certificates distribution scheme for vehicular cloud networks. *Security and Privacy*, 1(1):e11, 2018
15. Yuan Yao, Bin Xiao, Gaofei Wu, Xue Liu, Zhiwen Yu, Kailong Zhang, and Xingshe Zhou. Voiceprint: A novel sybil attack detection method based on rssi for vanets. In *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 591–602. IEEE, 2017.
16. Yuan Yao, Bin Xiao, Gaofei Wu, Xue Liu, Zhiwen Yu, Kailong Zhang, and Xingshe Zhou. Multi-channel based sybil attack detection in vehicular ad hoc networks using rssi. *IEEE Transactions on Mobile Computing*, 18(2):362–375, 2019.
17. Tong Zhou, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty. P2dap—sybil attacks detection in vehicular ad hoc networks. *IEEE journal on selected areas in communications*, 29(3):582–594, 2011.

AUTHORS PROFILE

Suhaib Rehman, M.E. Research Scholar, Department of Computer Science & Engineering, Chandigarh University, Mohali, Punjab, India.

Nitika Kaproor, Assistant Professor, Department of Computer Science & Engineering, Chandigarh University, Mohali, Punjab, India.