MAR_Sybil: Cooperative RSU Based Detection and Prevention of Sybil Attacks in Routing Process of VANET

Mahabaleshwar Kabbur[1] and Dr. V. Arul Kumar[2]
[1]Research Scholar, School of Computer Science & Applications, REVA University, Bengaluru
[2]Assistant Professor, School of Computer Science & Applications, REVA University, Bengaluru

Abstract. *VANET is a next generation communication technology where vehicles create an autonomous network with assistance of RSU (Road Side Units). VANET provides legitimate information to the users on the road, in order to increase the road and user's safety. It provides useful information to the vehicles about directions, location mapping, premises, etc. The fast propagation of emergency and local warning messages to the approaching vehicles will be helpful for preventing secondary accidents. If security of the network is not guaranteed, several attacks may occur, thereby alert messages may not reach to the RSUs on time or message may get spoof due to attack on it. Major attacks on emergency messages such as timing attack, spoofing attack, DoS attack, Sybil attack, etc. would be considered to mitigate and make the communication and infrastructure more secure. One of the major emergency message attack is Sybil, which is used by selfish message propagators to claim authenticity of their message by propagating with multiple identities. By deceiving other nodes with their false support using multiple identifies, they can achieve various purpose in network like vehicle re-routing, speed shift etc. This work proposes a RSU cooperative detection mechanism involving triangulation and fake propagation by RSU to identify the Sybil attacks in the VANET. The proposed methodology secures fast communication emergency messages to prevent secondary accidents by validating the message sources, nodes will accept only the messages from RSU which are digitally signed and source validated against Sybil nodes. The performance evaluation is made with existing methodology and effectiveness of the proposed methodology results demonstrated in article. The spatial location and trajectory of attacker is learnt effectively with RSU cooperation in the proposed work.*

Keywords: *VANET, RSU, Triangulation, Message Attestation*

1. Introduction

VANET has become a promising technology for vehicular communication, which communicates dynamically to exchange and share real time information between vehicles on roads. This technology enables variable infrastructure for emergency message communication to improve road safety for vehicles.

VANET technology can be used as real time alert systems to broadcast emergency messages to the police, ambulance and drivers of the vehicles in some unexpected situations like traffic emergency, accident, road conditions, vehicle tracking, whether conditions and message monitoring. This network architecture considers vehicles as nodes and information as packets for communication. Since these nodes operate in a physically insecure environment in the range of 100 to 300 meters circumference. The message communication will be done in Infrastructure to Infrastructure (I2I), vehicle to vehicle (V2V) and Vehicle to Infrastructure (V2I) environments.

Routing is the process of identifying, selecting and establishing a best shortest path for message communication. In order to provide required communication between source and destination, efficient routing mechanisms must be used. Security is a challenging issue for the technology to provide secured prominent approach for routing. We need to have a technology by virtue of which network nodes (vehicles) should be smart enough to manage

road safety at their own. The efficiency and safety level of transportation solution can be improved using it. Each vehicle has onboard wireless transmitter/receiver and the communication is further assisted with a Road Signal Units (RSU) deployed at various locations in roads. Vehicles can communicate with other vehicle directly or through multi hop manner using RSU and other vehicles in a path as relay. The autonomous characteristics of VANET expose itself to various security threats [1]. The VANET architecture and need of emergency message communication scenario is shown in figure 01.

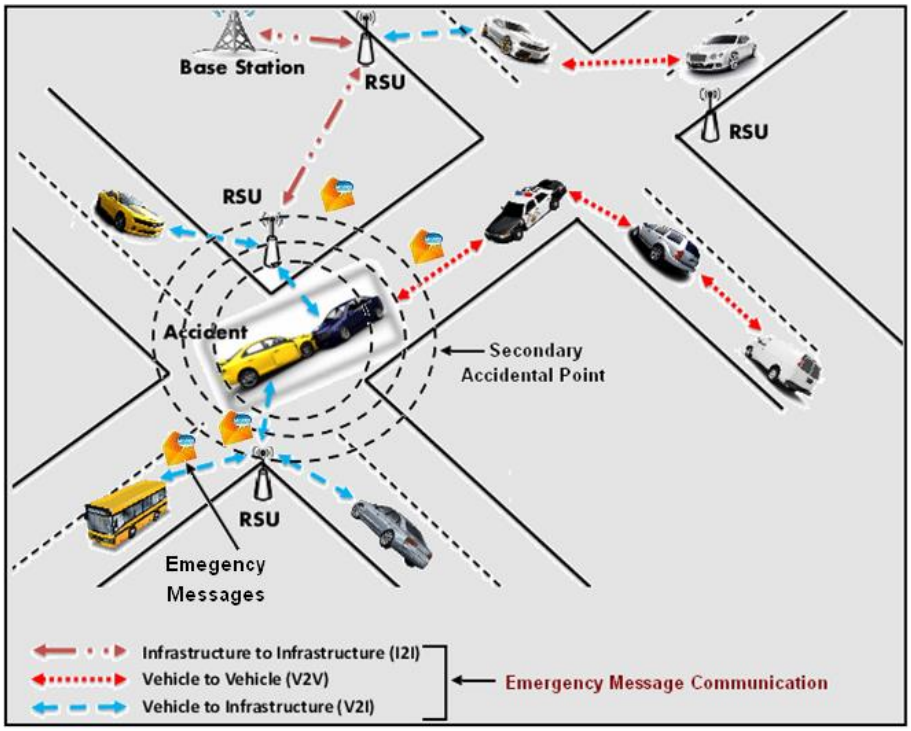


Figure 1: VANET Architecture and Emergency Message Communication Scenario

One of the major and challenging attack with respect to authenticity and identifications is Sybil attack. Where in Sybil attack vehicle claims multiple identities, which it learns through the messages propagated by other vehicles in the network. If network affected by Sybil attack then Sybil node will take control over the entire VANET. Sybil node may inject false emergency messages to the neighbouring nodes and creates accidents, secondary accidents and traffic congestion. As an example, a selfish driver can broadcast hello packets with different identities so as to create an illusion of traffic congestion and mislead other vehicles to take different paths.

In Figure 2 of Sybil Attack, the node claiming multiple identities are malicious nodes and the additional identities are Sybil nodes. Sybil attack detection approaches must identify the malicious node and prevent the effect of malicious node's messages propagated through its Sybil identities.

The existing solutions for Sybil attack detection in mobile ad-hoc networks; radio resource testing, identify registration and position verification does not work well for vehicular network. The assumption that simultaneous sending and receiving on same channel for radio resource-based attack detection does not hold in vehicular network as attackers can use multiple radios. With non-technical means of stealing identify registration-based attack detection is made ineffective. Due to high mobility, position verification approaches are not effective for vehicular network. This motivates to design new solutions for detection and prevention of Sybil attacks in vehicular network.

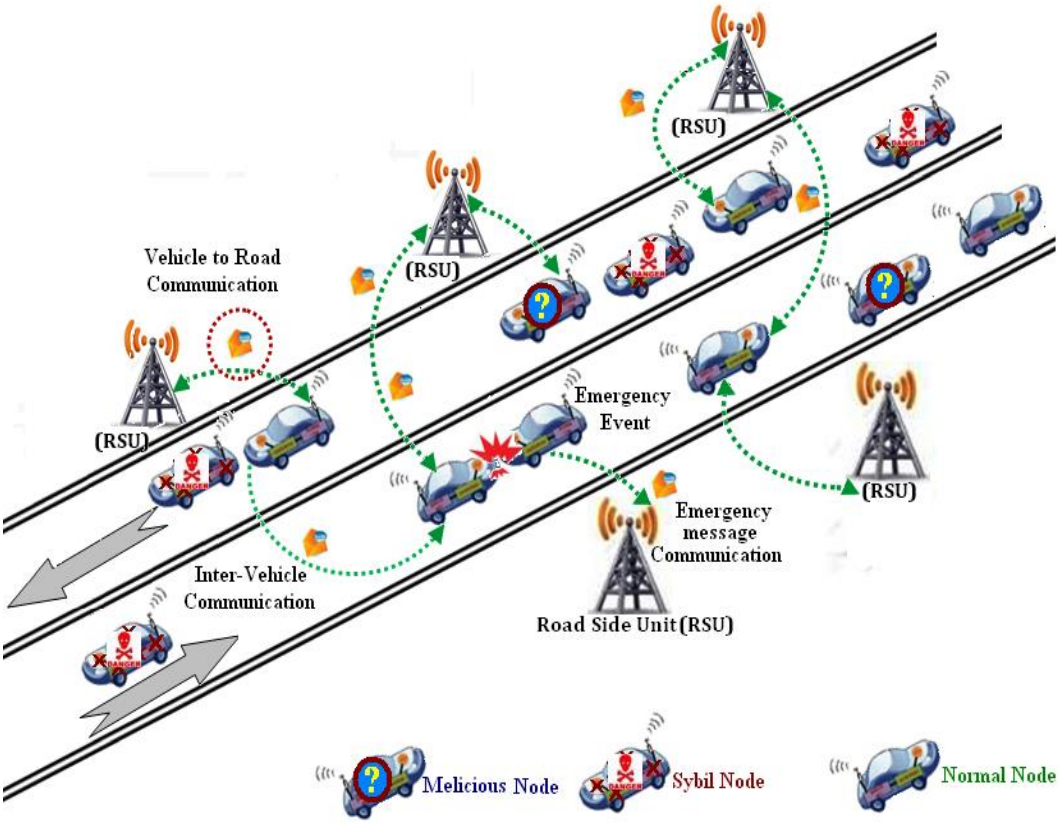


Figure 2: Sybil Attack in VANET

In this work we proposed a Sybil attack detection approach based on novel cooperation of multiple RSU is proposed. The spatial location of the malicious node, its spatial trajectory and the identify diversity of it can be learnt effectively using the proposed approach. The learnt identified diversity is used as signature for accurate detection of trajectory of the malicious node. Sybil attack scenario is shown in Figure 2.

2. RELATED WORK

Al-Mayouf et al. [1] designed and developed a strategy for addressing the shortcomings of creating an efficient routing protocol for attaining a globally optimal vehicle control. This problem elevates when various drivers have various unique preferences. This research focuses on establishing an efficient accident management system with the help of vehicular ad hoc networks. It leverages on the existing systems that uses cellular technology in public transport. Additionally, the accident management system is known to be effective in reducing magnitude of time needed to alert an ambulance which is the first thing needed at an accident site. This is generally accomplished by using a multi-hop optimal forwarding algorithm.

In [1], trajectory is created in form of sequence of RSU visited. The similarity between two trajectories is calculated as,

$$Sim(T_1, T_2)\begin{cases} -1 & postive\ test \\ \dfrac{|T_1 \cap T_2|}{Min\{|T_1|, |T_2|\}} & negative\ test \end{cases}$$

Similar trajectories are analysed for presence of Sybil attack. The approach does not work well when malicious node mutes certain identities. Based on Boneh-Shacham (BS) short group signature scheme and batch verification, Sybil attacks are detected

D. S. Reddy et.al.[2] proposed neighbour information-based Sybil node detection and dynamic certificate scheme-based protection against attack. Each node advertises its neighbours' lists learnt from beacons to the RSU. Sybil nodes will have same neighbour list. Based on analysis of the neighbour list, the Sybil nodes are detected by intersecting the neighbour list over time for a node and thresholding the appearance of the node more than certain time.

$$R = N_v^{t_0} \cap N_v^{t_1} \cap N_v^{t_2}$$

$$\prod_{x=1}^{|R|} |x| > T, x \; is \; sybil$$

In addition, short pseudo lived certificates are provided by RSU and vehicles accept only RSU certified messages. The solution can be deceived by the attacker by careful scheduling of fake identities and the interval between them. Also, the approach fails when capture and replay attack is launched in the network. Event based reputation system is proposed in [2] to detect Sybil attack and suppress spread of false information. Every event in VANET is assigned as reputation and trust score. Only events whose reputation and trust crosses a threshold; it is notified to vehicles. The calculation of reputation and trust is done considering the flooding time of the event within a window time. Same event appearing after the window time is dropped for trust calculation. This method fails for the case of multiple radios where malicious node can flood events at same time.

Thi Ngoc Diep Pham [3] proposed more secured and flexible platform for VANET nodes to manage trust and privacy. First, they implemented ALRS (A Secure Link Ability Scheme) to recognize the vehicle nodes or trust levels of other nodes in VANET. The link identification information is kept confidential for all attackers using encryption and private set intersection technique. Second, they implemented ATMS (a context-Aware Trust Management Scheme) that allows vehicles to analyse the trustworthiness of accepted actions by considering the entity strength of the sender. In the context of privacy, accessing trust value of an entity is the very challenging job. To overcome the problem of challenge scenario linkability content is used in ALRS and developed decision tree to estimate the trust of an entity.

Mohamed S. Mohamed et al. [4] Sybil attack detection based on the observation of BSM (Basic Safety Message) in DSRC (Dedicated Short-Range Communications) safety applications. Based on the pattern of BSM messages provided by vehicular node, Sybil attack is detected.

S. Chang et al. [5] designed aggregate emergency message authentication (AEMA) technique to identify and evaluate an information emergency event. This mechanism represents syntactic aggregation and cryptographic aggregation techniques to minimize the data transmission cost for VANET nodes and to minimize un authentication and to maintain the efficiency of emergency messages using batch verification technique

Yuan Yao et al. [6] RSSI (Received Signal Strength Indicator) based Sybil attack detection is proposed. RSSI values over a period of time is aggregated as time series and compared against all the series for anomaly analysis. Based on the anomaly Sybil attacks are detected. RSSI time series for different node behaviours are displayed below.

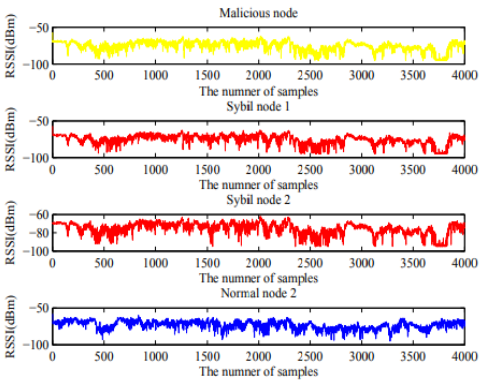


Figure 3: RSSI Series [6]

From the results, the RSSI series of Sybil nodes is found to exhibit a similar pattern different from that of others. Based on traffic density the pattern regularity changes and need complex DWT features to detect attacks. Trajectory of vehicles is captured in form of footprint and the footprint is compared to detect Sybil attacks [7]. The trajectory is created in form of sequence of RSU visited. The similarity between two trajectories is calculated as,

$$Sim(T_1, T_2)\begin{cases} -1 & postive\ test \\ \dfrac{|T_1 \cap T_2|}{Min\{|T_1|, |T_2|\}} & negative\ test \end{cases}$$

Similar trajectories are analysed for presence of Sybil attack. The approach does not work well when malicious node mutes certain identities. Based on Boneh-Shacham (BS) short group signature scheme and batch verification, Sybil attacks are detected in [8]. Each vehicle must be registered in a group of related RSU before V2V communication. RSU authenticates applicant vehicle and provide group private key to communicate with legitimate vehicle in group. By this way it can identify any malicious node, but the condition of creating group registration before communication for every transit though RSU is not practically possible.

Aravendra Kumar Sharma. [9] Event based reputation system is proposed to detect Sybil attack and suppress spread of false information. Every event in VANET is assigned as reputation and trust score. Only events whose reputation and trust crosses a threshold, it is notified to vehicles. The calculation of reputation and trust is done considering the flooding time of the event within a window time. Same event appearing after the window time is dropped for trust calculation. This method fails for the case of multiple radios where malicious node can flood events at same time.

R. Shrestha et al. [10] says that Received Signal Strength (RSS) value measured by each vehicle to who it communicated is compared to detect the Sybil attacks. Each vehicle measures the signal strength of the vehicle it communicates and a signal vector is created for each as,

$$V_i = \{S_1^i, S_2^i, S_3^i, \dots S_n^i\}$$

The distance between two signal vectors is measured using Euclidean formula as,

$$|V_i - V_j| = \sqrt{(S_1^i - S_1^j)^2 + (S_2^i - S_2^j)^2 + \cdots (S_n^i - S_n^j)^2}$$

V_i, V_j are assumed as same nodes if their signal vector distance is less than a threshold.

$$|V_i - V_j| < \lambda$$

The attacker can deceive the approach by selectively using the identities and this approach is high dependent on the mobility model.

3. PROPOSED SOLUTION

The proposed solution consists of three parts

3.1. Detection of Sybil Node
3.2. Detection & Tracking of Malicious Node
3.3. Prevention from Fake Messages

3.1. Detection of Sybil Node

The proposed solution places the RSU in such a way that the position of any vehicle can be found using triangulation. In triangulation pattern, first RSU represents RSU_1(X1, Y1), second RSU represents RSU_2(X2, Y2) and third RSU represents RSU_3(X3, Y3) to identify the location of vehicle. The triangulation cross section position of three RSU's indicates the position of vehicle as Vehicle (X, Y). The distance between the RSU and the vehicle i.e., distance between the antennas of reference RSU and transmitting RSU is measured based on

Radio Signal Strength (RSS) and represented as d1, d2 and d3. RSS is measured in terms of *dBm*- DeciBels / *milliwatt*. The proposed algorithm of Sybil attack detection is shown below.

START

Step 1. [Identify the location of vehicle from 3 RSUs]
RSU_1(X1, Y1), RSU_2(X2, Y2) & RSU_3(X3, Y3)

Step 2. [Calculate the position of a vehicle from three RSU's, based on triangulation pattern]

Step 3. Vehicle position in is triangulation pattern is Vehicle (X, Y)

$$x = \frac{CE - FB}{EA - BD}$$

$$y = \frac{CD - AF}{BD - AE}$$

Step 4. Triangulated location of a node with time stamp is broadcasting to the neighboring nodes.

Step 5. Identify and finalize, conflicting position of a node for same time stamp as Sybil node.

STOP:

Algorithm 1: Sybil Node Detection Algorithm

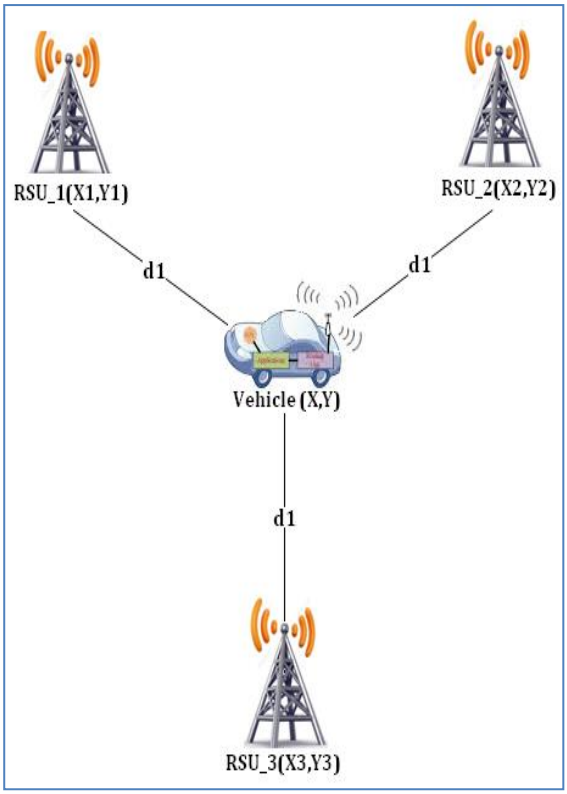


Figure 4: Structure of Triangulation Pattern

The architecture of triangulation pattern is shown in Figure 4. The triangulated location of proposed methodology is calculated as follows

$$d = k * \sqrt{RSS}$$

Where,

d= Distance between RSU and Vehicles
k= Constant
(Indicates Frequency of radio signal protocol)
RSS= Radio Signal Strength

The triangulated location of vehicle (x, y) is calculated as

$$x = \frac{CE - FB}{EA - BD}$$

$$y = \frac{CD - AF}{BD - AE}$$

Where,

$A = -2x_1 + 2x_2$
$B = -2y_1 + 2y_2$
$C = r_1^2 - r_2^2 - x_1^2 + x_2^2 - y_1^2 + y_2^2$
$D = -2x_2 + 2x_3$
$E = -2y_2 + 2y_3$
$F = r_2^2 - r_3^2 - x_2^2 + x_3^2 - y_2^2 + y_3^2$

In proposed architecture every message sent by a node with its identifier, RSU cooperatively triangulates the position of the node. Each RSU attaches timestamp to the triangulated location of node and broadcasts to

neighbouring RSU's. RSU detects conflicting position of node for same time stamp as the Sybil node. Figure 05 shows Detection of Sybil node in triangulation pattern.

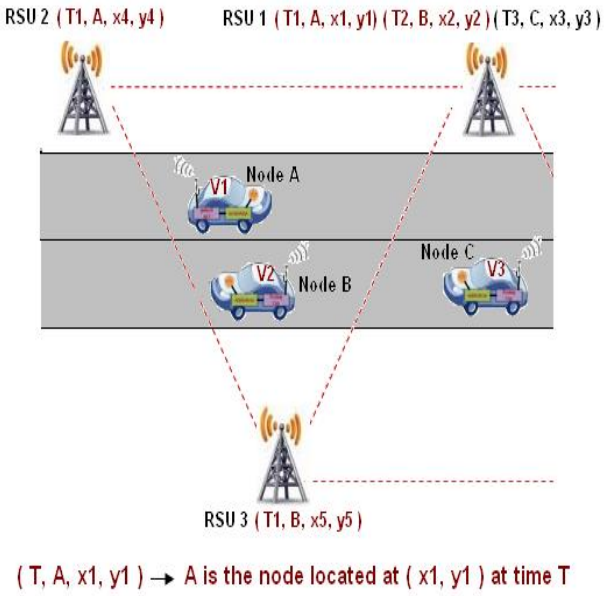


Figure 5: Detection of Sybil Nodes

From the time stamped node, position tracked at each RSU above, then node A, B is found to be Sybil node at RSU1.

3.2. Detection & Tracking of Malicious Node

In previous mechanisms [6][7] it's very difficult to identify or track the malicious node. The algorithm for Sybil attack detection & tracking of malicious node is given below.

START:

Step 1. Construction the appearance vector of nodes viewed over time period

Step 2. Identify the diversity pattern of the malicious node

$T1 \rightarrow \{A, C, D, E\}$

$T2 \rightarrow \{B, C, F\}$

$T3 \rightarrow \{A, D, F\}$

$T4 \rightarrow \{B, C, E\}$

$Sybil\ Nodes = \{A, B, E, F\}$

Step 3. Identify the position of vehicle which is alternating across set in same time slot.

Step 4. Confirm the node as malicious only if, node alternating across the set over the period.

STOP:

Algorithm 2: Malicious Node Detection and Tracking Algorithm

In proposed system, RSU keeps tracks of the messages from the Sybil nodes and constructs an appearance vector of nodes viewed over time period in term of window interval. With Sybil nodes detected in earlier stage, the appearance pattern of Sybil nodes in appearance vector over time period, provides the identify diversity pattern of the malicious node from the series of appearance vector below

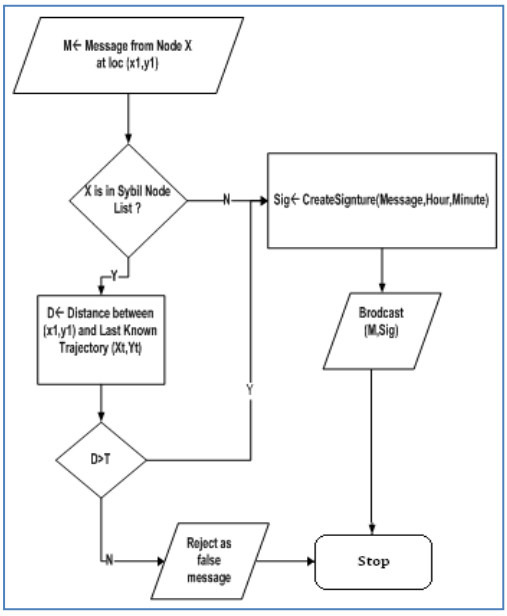
$$T1 \rightarrow \{A, C, D, E\}$$
$$T2 \rightarrow \{B, C, F\}$$
$$T3 \rightarrow \{A, D, F\}$$
$$T4 \rightarrow \{B, C, E\}$$
$$Sybil\ Nodes = \{A, B, E, F\}$$

It can be found that there are two malicious nodes with one alternating across the set $\{A, B\}$ and another alternating across set $\{E, F\}$ for fake message distribution. The position of node set $\{A, B\}$ and $\{E, F\}$ over the period of time is the trajectory of the malicious nodes.

3.3. Prevention from Fake Messages

In the proposed solution a private public key pair is generated and the private key is distributed to all the RSU and public key is distributed to all the vehicles shown in figure 06. In VANET infrastructure Private and Public keys act like identification parameters for all vehicles belonging to the network.

In VANET, once a vehicle identifies as a node of the network, digital signature authentication technique is applying on each node for message communication. Each vehicle of a network doesn't process any message without digital signature and rejects it as a fake message of Sybil Node. In the proposed system current minute and hour is used as digital signature parameters for the authentication. Once a vehicle sends a message to RSU, RSU checks the originator of the message for its presence in Sybil node. If the originator is not a Sybil node, then RSU creates a digital signature with its current minute and current hour. Once a vehicle is digitally signed then RSU creates a signed message for the authentication with message content and signature, then it broadcasts in the RSU area of the VANET. The vehicular node which is receiving the message authenticates the signatures [checks whether it is signed by RSU] by accepting the message for valid signature.



Flowchart 1: Flowchart of Trajectory Measurement Through RSU

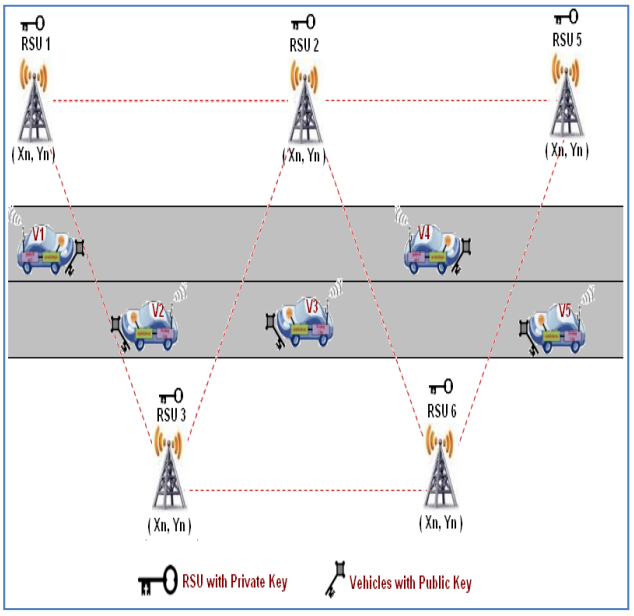
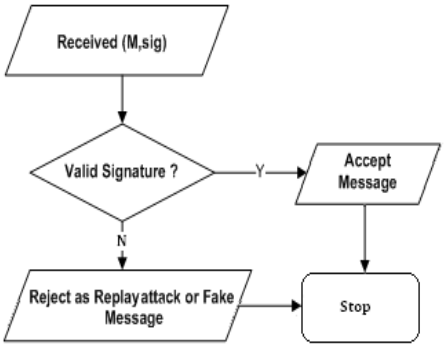


Figure 6: Triangulation Structured VANET Architecture with private public key pair

In the proposed system replay attacks launched by capturing a message and propagating at later time will fail. If the originator is a Sybil node, in this case the distance of Sybil node current position to its last known position of trajectory is measured. If the distance (D) is lesser than threshold (T) then the message is rejected as fake, or else (if the distance is greater than threshold) it will be actual message received from valid node. After the confirming, originator node is not a Sybil node then the message is digitally signed with parameters as

mentioned previously and broadcasted. The behaviour of the RSU is given in below flow chart. The behaviour of the vehicular node on reception of message is demonstrated in the flow chart below.



Flowchart 2: Data Reception flow chart

4. RESULTS

The proposed solution was tested for following VANET topology with RSU at every corner shown in Figure 7. The simulation was conducted through given configurations shown in table 1.

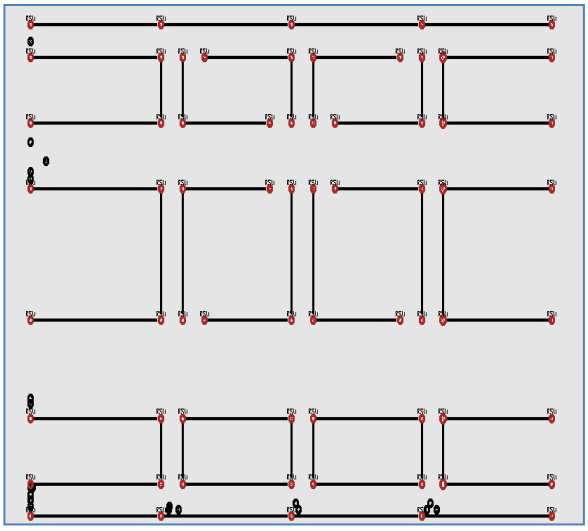


Figure 7: Simulation Topology

Number of Vehicles	100 to 500
Number of Malicious nodes	10% of Number of Vehicles
Number of identifies used by Malicious node	5
Simulation Duration	10 minutes
Vehicle Speed	30 m/ second
Fake Message rate	10 messages / second
Simulator	NS2
Area of Simulation	1000 m * 1000 m
Routing Protocol	AODV

Table 1: Simulation Configuration

The performance of the proposed solution is measured in terms of

- Attack Detection Ratio
- Fake Message Rejection Ratio
- Attack Detection Accuracy
- Attack Detection Time

Attack Detection Ratio (ADR) is the number of malicious nodes detected per minute. It is given as,

$$ADR = \frac{No\ of\ Malicious\ Detection}{Simulation\ time\ in\ minutes}$$

The performance of the proposed solution is compared against RSSI based detection approach proposed in [6] is given in figure 08. The attack detection ratio is measured by varying the number of vehicles and malicious nodes shown in table 02 and the result is given below.

No of Vehicles	Proposed RSU Cooperative Scheme	RSSI Based
100	05	04
200	10	07
300	14	11
400	18	15
500	24	20

Table 2: Comparison of Attack Detection Ratio

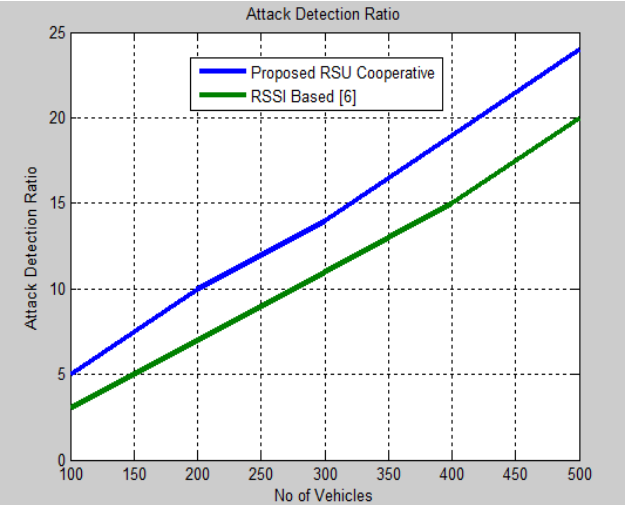


Figure 8: Comparison of Attack Detection Ratio

Fake Message Rejection Ratio (FMRR) is the number of fake messages detected and dropped for every minute interval. It is given as

$$FMRR = \frac{No\ of\ Fake\ Messages}{Simulation\ time\ in\ minutes}$$

The fake message detection ratio is measured by varying the number of vehicles and malicious nodes and the result of the proposed system given in figure 9.

No of Vehicles	Proposed RSU Cooperative Scheme	RSSI Based
100	20	12
200	42	30
300	60	50
400	90	80
500	120	110

Table 3: Fake Message Detection Ratio

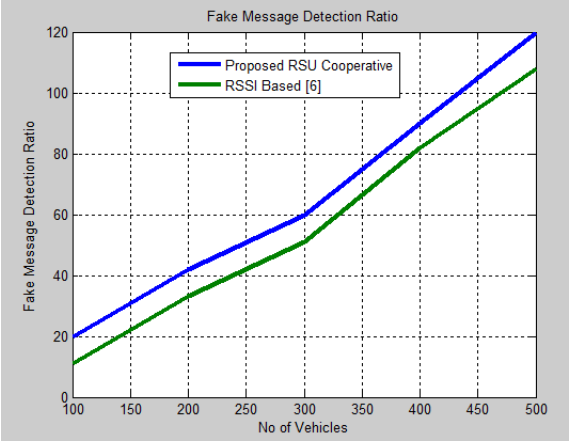


Figure 9: Comparison of Fake Message Detection Ratio

From the results, it can be seen that the fake message detection ratio is higher in the proposed solution compared to [6] and the fake message detection ratio in the proposed RSU cooperative scheme is 9% higher than RSSI based scheme.

Attack Detection Accuracy (ADA) is the ratio of detected attackers out of total attackers in the network.

$$ADA = \frac{No\ of\ Detected\ Attackers}{Total\ Attackers} * 100$$

The attack detection accuracy is measured by varying the number of vehicles and malicious nodes and the result is given in Figure below.

No of Vehicles	Proposed RSU Cooperative Scheme	RSSI Based
100	87	65
200	88	73
300	90	76
400	91	80
500	92	82

Table 4: Attack Detection Accuracy

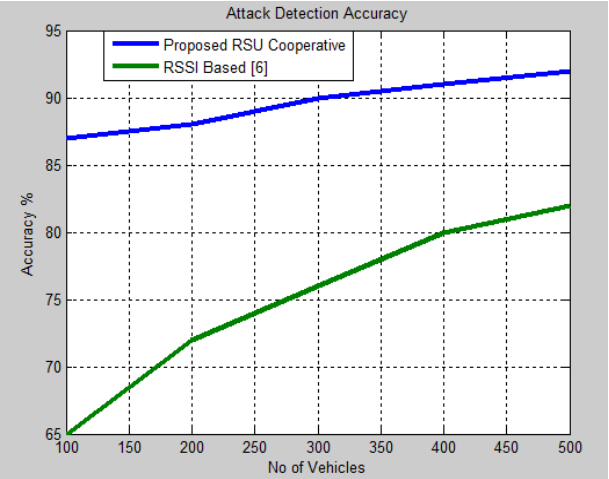


Figure 1: Comparison of Attack Detection Accuracy

From the result, it can be seen that the fake accuracy is higher in the proposed solution compared to [6]. The fake detection accuracy is 12% more in proposed RSU cooperation scheme compared to RSSI based scheme.

Attack Detection Time is the times at maximum number of attackers are detected in the network.

The attack detection time is measured by varying the number of vehicles and malicious nodes and the result is given figure 11.

No of Vehicles	Proposed RSU Cooperative Scheme	RSSI Based
100	2	4
200	3	8
300	3	13
400	4	15
500	5	16

Table 5: Attack Detection Time

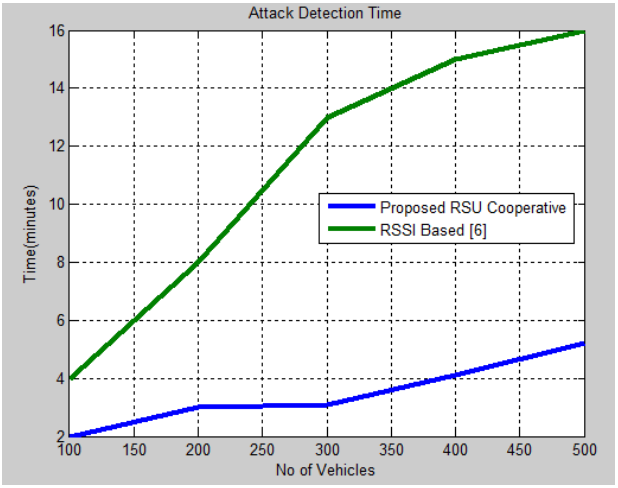


Figure 2: Comparison of Attack Detection Time

From the result, it can be seen that the attack detection time is lower in the proposed solution compared to [6]. The proposed RSU cooperative scheme has 68% lower attack detection time compared to RSSI based scheme.

5. CONCLUSION

RSU Cooperation based Sybil attack detection is proposed in this work. The position of nodes learnt using triangulation. This location is communicated across RSU to identify the conflict in location for the same timestamp to detect Sybil nodes. With the list of detected Sybil nodes and their pattern of appearance in each RSU coverage area, the trajectory of the malicious node and its identity varsity is detected. By validating the message sources, vehicles will accept only messages from RSU which are digitally signed and source validated against Sybil nodes. The effect of fake messages is reduced in proposed methodology of the network. The

performance results demonstrated the effectiveness of the proposed solution against [6]. The approach can be further improved to reduce the false positives and use of machine learning algorithm for identity varsity detection and trajectory tracking.

REFERENCES

[1]. Al-Mayouf, Y. R. B., Mahdi, O. A., Taha, N. A., Abdullah, N. F., Khan, S., &Alam, M. "Accident Management System Based on Vehicular Network for an Intelligent Transportation System in Urban Environments". IEEE ISCISC Journal of Advanced Transportation, 2018.
[2]. D. S. Reddy, V. Bapuji, A. Govardhan, and S. Sarma, "Sybil Attack Detection Technique Using Session Key Certificate in Vehicular Ad Hoc Networks," in Proc. IEEE ICAMMAET, 2017, pp. 1–5.
[3] Thi Ngoc Diep Pham, Chai Kiat Yeo., "Adaptive trust and privacy management framework for vehicular networks". *Vehicular Communications, 13,* pp.1-12, ELSEVIER 2018
[4]. Mohamed S. Mohamed; Prajjwol Dandekhya; Axel Krings "Beyond passive detection of sybil attacks in VANET", International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), IEEE 2016.
[5] H. Zhu, X. Lin, R. Lu, P. -. Ho and X. Shen, "AEMA: An Aggregated Emergency Message Authentication Scheme for Enhancing the Security of Vehicular Ad Hoc Networks", IEEE International Conference on Communications, Beijing, pp. 1436-1440, 2018.
[6] Yuan Yao; Bin Xiao; Gaofei Wu; Xue Liu "Multi-channel-based Sybil Attack Detection in Vehicular Ad Hoc Networks using RSSI", IEEE Transactions on Mobile Computing May 2018.
[7]. S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, "Footprint: Detecting Sybil Attacks in Urban Vehicular Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 6, pp. 1103–1114, 2012.
[8] M. Alimohammadi and A. A. Pouyan, "Sybil Attack Detection Using a Low-Cost Short Group Signature in VANET," in Proc. IEEE ISCISC, 2015, pp. 23–28.
[9] Aravendra Kumar Sharma "Sybil Attack Prevention and Detection in Vehicular Ad hoc Network", International Conference on Computing, Communication and Automation (ICCCA), IEEE -2016.
[10] R. Shrestha, S. Djuraev, and S. Y. Nam, "Sybil Attack Detection in Vehicular Network based on Received Signal Strength," in Proc. ICCVE, IEEE (2014), pp. 745–746
[11] Yuan Yao; Bin Xiao; Gaofei Wu; Xue Liu "Multi-channel-based Sybil Attack Detection in Vehicular Ad Hoc Networks using RSSI", IEEE Transactions on Mobile Computing May 2018.
[12] Xia Feng,Chun-yan Li "A method for defensing against multi-source Sybil attacks in VANET", Peer-to-Peer Netw. Appl. Springer (2017).
[13] Yuan Yao; Bin Xiao; Gaofei Wu; Xue Liu "Multi-channel-based Sybil Attack Detection in Vehicular Ad Hoc Networks using RSSI", IEEE Transactions on Mobile Computing May 2018.
[14] Jie Cui, Xuefei Tao, Jing Zhang,Yan Xu and Hong Zhong "HCPA-GKA: A hash function-based conditional privacy-preserving authentication and group-key agreement scheme for VANETs" ELSEVIER, 2214-2096 - 2018.
[15] Thi Ngoc DiepPham & Chai KiatYeo,"Adaptive trust and privacy management framework for vehicular networks", ELSEVIER, 2214-2096/ 2018.
[16] A. Boualouache, S. M. Senouci, S. Moussaoui, A survey on pseudonym changing strategies for vehicular ad-hoc networks. IEEE Commun. Surv. Tutor. 20(1), 770–790 (2018)
[17] H. Li, R. Lu, J. Misic, M. Mahmoud, Security and privacy of connected vehicular cloud computing. IEEE Netw. 32(3), 4–6 (2018)
[18]. J. Qiao, Y. He, X. S. Shen, Improving video streaming quality in 5G enabled vehicular networks. IEEE Wirel. Commun. 25(2), 133–139 (2018)
[19]. Mujeeb Ur Rehman, Sheeraz Ahmed, Sarmad Ullah Khan, Shabana Begum, and Atif Ishtiaq, "ARV2V: Attack resistant vehicle to vehicle algorithm, performance in term of end-toend delay and trust computation error in VANETs," in 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), pp. 1–6, Sukkur, Pakistan, 2018, IEEE.
[20] Mr. Mahabaleshwar Kabbur & Dr. V. Arul KumarS, "Detection and Prevention of DoS Attacks in VANET with RSU's Cooperative Message Temporal Signature" in 2019 IJRTE ISSN: 2277-3878.