International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

Defending Against Sybil Attacks by Enhanced Event Based Reputation System in Vanet

Kunal J. Dutt, Seema B. Joshi

Abstract: - In earlier times, vehicles were the realm of mechanical & automobile people, but with proliferation of computer technology & electronic components, vehicles are becoming "Computer on Wheels". These technology lies in VANET (Vehicular Ad-Hoc Network) environment.

VANET has various road safety applications, with the aim of communication interoperability between cars. In VANET, Sybil attack have been reckon as a major threat, by creating illusion or traffic congestion, it may lead mass destruction. Previously Event Based Reputation System (EBRS) named technique has been used to defend this Sybil attacks, but there was one major drawback that they were not considering RSU and TA modules security. For these both modules assumption has been made that it cannot be compromised thus it is trustable. But in this way VANET environment cannot be established thoroughly .In this paper we proposed enhance Event Based Reputation System to defend Sybil attacks in VANET environment, which is going to eliminate that major assumption by considering RSU and TAs security mechanisms.

Keywords: - EBRS, Sybil attack, Sybil in VANET, VANET, VANET Security,

I. INTRODUCTION

VANET was introduced in 2001, under "car to car ad-hoc network"[1]. It is an important segment of ITS (Intelligent Transport Systems).VANET has been derived from principles of MANET[2], with certain modifications,VANET contains vehicle embedded with sensors which are treated as a mobile nodes, road side units which would be considered as fixed infrastructure and wireless interconnection to allow them to communicate with each other.[3]. VANET's main goal is to achieve more safe and convenience drive. Apart from safety, there are many non-safety applications, such as Internet access, weather forecast, geo-location can enhance driving experience by getting ease, convenience and infotainment.[4]Two communications modules are defined in VANET, one is V2V (Vehicle to vehicle) communications whereas other is V2I (Vehicle to Infrastructure)[5], as illustrated in figure 1.

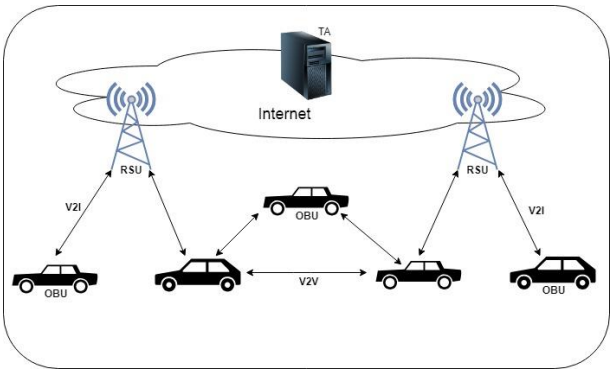

Figure 1 VANET Architecture

But more features invites more risks too. There are various attacks that can take place in VANET environment and lead to mass destruction. In this research paper we are going to talk about one of the major attack, which is Sybil attack. When malicious vehicle node is capable to pretend as multiple vehicles, it is defined as Sybil attack in VANET.[6] Sybil attack was proposed by John R. Douceur, in terms of peer to peer networks.[7]. Sybil attack may lead to momentous threats by sending fake messages, notifications and fabricating traffic outline. Sybil attack can give the attackers genuine legitimate identity. Sybil attack is a kind of attack which cannot be eliminated thoroughly, but destruction caused through Sybil attack can be mitigated by detecting Sybil nodes as early as possible.[7] There are many methods available for Sybil detection but they all are having certain limitations and constraints, so they cannot give sufficient up to the mark resolutions[8][6].

In this paper, we present an enhanced Event based reputation system to defend Sybil attack. Earlier event based reputation system[9] has been proposed by Xia Feng et el. Which was far better than other methods like, RSSI (Received signal strength indicator) detection method, resource testing approach method, time stamp series approach etc. But it has been built on one major assumption that, TA & RSU cannot be compromised. Which is making VANET security incomplete in terms of communication security. So we are going to proposed enhanced event based reputation system, which is going to provide not only V2V security but it will also consider the V2I security, which is not considered in existing method.

II. MODELS AND DESIGN GOALS

A. System Model

Here figure 1 illustrates the architecture of Vehicular ad-hoc networks.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
Kunal J. Dutt, GTU-School of Engineering & Technology, Gandhinagar, India.
Seema B. Joshi, Assistant Professor, GTU-School of Engineering & Technology Gandhinagar, India.

In this architecture, there are vehicles, Road Side Units (RSU) and server. Each particular vehicle is having configuration of On Board Unit (OBU), which is going to be used in information transmissions, and warning notifications. RSUs is taking role of entry point in this system. It will produce local certificate to each vehicle. To start communication after certificate generation, there is certificate validation which is going to be done with the help of TA. Which is distributor of certificates in our system. There is a table to store information in three columns having names, sender vehicle list, receiver vehicle list and list of activity which takes place between sender vehicle and receiver vehicle. This table is stored by RSUs..

B. Attack Model

Sybil attack tries to forge identity and it can counterfeit the traffic scenario by sending false messages with multiple identities, which habitually leads to traffic jam and accidents full of destructions.[6]. Sybil attack is an attack, which cannot be eliminated thoroughly from the environment[10], but by certain mechanism we can mitigate the destruction caused by it. Here in given system if Sybil or malicious node has been sent from the initial RSU, it will accomplish authentication and procedure and enter in the VANET environment's territory. By the time this malicious node would get reputation value increment as it is coming from the initial point, where one major assumption has been done that RSU and TA cannot be compromised. So in this kind of Sybil attack malicious node can even be legitimate by the time of increment of its reputation value, which is the mechanism currently applied to securing V2V security. But it is not sufficient and efficient method to reduce Sybil's destructions. Once it may enter in the VANET territory it will get more and more authenticated legitimacy. This leads to a Sybil node transformation in to a legitimate node and causes mass destruction. Unless it is not detected and removed from the consideration.

C. Design Goals

To wangle the problems in extant Sybil attack detection approaches and above attack model, we prompt an enhanced Event Based Reputation System. Our system will keep all the goals of current EBRS and in addition it will give more secured mechanism it will compare hash values instead of reputation values as it may violate at certain cases(if malicious node has been entered from initial RSU). Here major design goal behind this mechanism is to eliminate the illusions created by malicious node/car to mitigate the destruction caused by wrong traffic information.

III. PROPOSED ENHANCED EVENT BASED REPUTATION SYSTEM

By following current work flow of EBRS, mandatory steps like Certificate generation & validation would be same.in our proposed method we have included a thing which is not mentioned in entire process, RSU. Here in our system RSU would create event log with hash values to to justify authenticity of event and nodes, who're performing that particular event. By this detection of false/fake events performed by attackers, our Sybil nodes can be identified. Here those hash values will be compared between different RSUs and if their hash values are coming different from previous, it can be event performed by illegitimate vehicle nodes

A. Methodology of Enhanced EBRS

Steps

1 certificate generation

2 Certificate Validation

3 Data Comparison between two RSU to eliminate the malicious node

1. Certificate generation

Every vehicle which is going to be the part of VANET environment, must require to generate certificate with several credentials details. This would be first step in this system and its working would be same as previously designed EBRS. In prior design they were allocating dynamic reputation value and trusted value. Here we are going to consider and integrate unique hash values for each vehicle to distinguish themselves among other vehicles and apart from that, it would maintain privacy of car details too. This generated data would be stored by initial RSU entry point. This all credentials would be generated under Trust Authority module.

Vehicle would send its basic details to RSU, RSU would forward it towards TA. TA would generate confirmation message upon given credential details and it would pass back with certificate with credentials. This certificate would be consider as a authenticated document by TA to participate in further VANET communication in VANET environment.

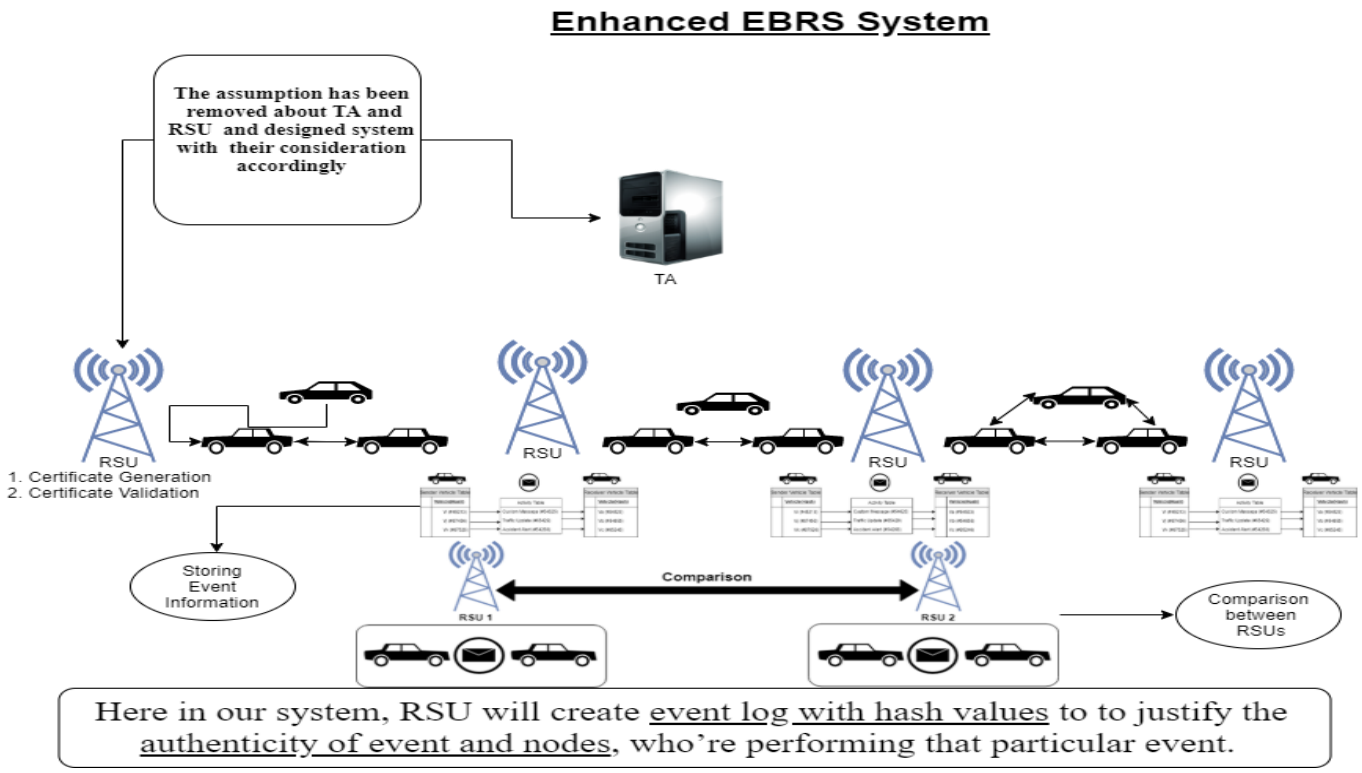

Figure 2 Methodology Diagram of Enhanced EBRS

2. Certificate Validation

Once vehicle get their local certificate it is able to perform communication with other registered vehicle roaming in traffic network. To gain trust and authenticity receiver vehicle would validate the sender vehicle's certification with the help of RSU and TA which are responsible for certificate generation and allocation to individual vehicles.

In this procedure, initially when receiver will get message from sender's vehicle, receiver would send those details towards RSU and it would check its authenticity and respond back to receiver vehicle whether it is on list legitimate vehicle or malicious node. It would be happen with the hash integrity check between two RSUs if it is matching with the RSU's list, it would be taken in consideration as it would be eliminate from the consideration in communication between vehicles.

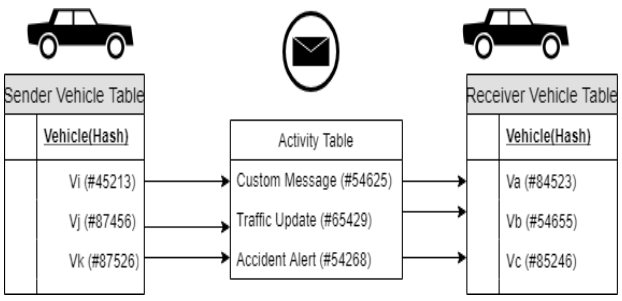

Figure 3 Storing event Information

In RSU there would be structure stored as above figure illustrates, there would be 3 table in sequence, sender vehicle table which would have details of vehicle with its hash numbers column, next it would have activity table which would store name of activity along with its allocated hash number, and lastly receiver vehicle table, which would have same columns as sender vehicle table, vehicle name along with hash number.

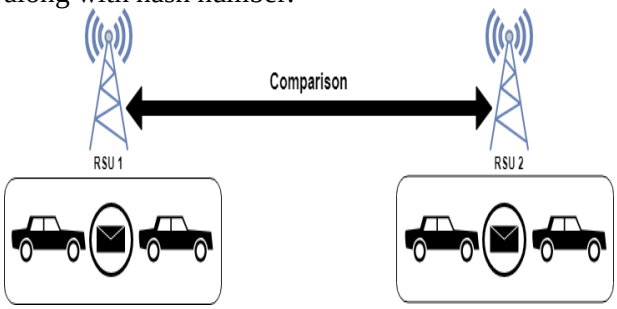

Figure 4 Comparison between RSUs

Among illustrated table would be stored by each individual RSUs. After that to authenticate malicious Sybil nodes activity, it would perform comparison test between stored data between RSUs. This can be relate as a activity logs, which will have sender and receiver vehicle data and activity which has been taken place among those two vehicles. These table's entity names would have attached hash values to be compare with next RSU's table to detect Sybil nodes. If nodes would be legitimate there would be no changes during the journey, there hash values would be same through the entire journey. But if we take one scenario where after initialization and entering in the VANET environment, Sybil node has been illustrated or forged by taking some legitimate node's identity and by using that identity malicious node may create illusions, but by considering hash based logs, those malicious Sybil node would not having legitimate hash value as original one.

From that it may be identified or detected that it is Sybil node, this is how it can be eliminated from the consideration to mitigate the destruction caused from Sybil attack.

B. Steps of procedures of Proposed Enhanced EBRS.

1. Certificate Generation
2. Certificate Validation
3. Generating Event tables at RSUs
   3.1 Storing hash values of Sender vehicle table
   3.2 Storing hash values allocated to activity performed
   3.3 Storing hash values of Receiver Vehicle table
4. Comparing with up next RSUs Event table.
5. If hash value mismatch/missing, that node would be counted as Sybil node
6. Elimination of detected Sybil Node.

IV. COMPARISON ANALYSIS WITH RELATED WORK

In the base paper Xia feng et al defined more than 5 methods and put up comparison analysis of 3 among those 5 related mentioned methods. This analysis was covering one major thing that except EBRS, none other method was able to defeat Conspired Sybil attack. Here we are taking those parameters and considering few more Parameters, which has been mentioned in comparison analysis table. They compared their EBRS method with 3 other methods, which are Similarity of neighboring information (SNI), Time Stamp Approach (TSA) and Received Signal Strength Indicator (RSSI).

A. RSSI method:-

Each and every vehicle would have one individual single identity and this single identity cannot be located at more than one place, this fundamental was origin and inspiration behind the RSSI technique[11][12]. So if the identity of a vehicle node and its location/position are bound together, they would be able to detect the Sybil
Attack. Many researchers came up with the method of RSSI by estimating node's position. They explicate that, if two messages are having the same estimated position, they deduce that they are from the same node, which is Sybil attacker
Yu[11], got the measure of estimated nodes positions by implement predetermined signal propagation model and RSSI to verify the accuracy of location information. A node is considered suspect if it's claimed position/location is too far from the evaluated one.
Boussia[11] estimated the RSSI range of next message using Friss Free Space path Loss Model. If the real RSSI of next message is out of range (from defined/gained), they regard the sender is a Sybil vehicle.
This RSSI based technique were having limitations which was giving red signal to its deployment towards the end users. Detection accuracy is limited, because of that signal strength may be influenced by complex road conditions. One more limitation is that this method cannot defend against conspired Sybil attack.

B. Time stamp Approach

Taking RSUs as references, the vehicles generate their movement trajectories. By comparing and computing those vehicle's movement trajectories, Sybil attacks can be detected, this approach is known as TSA[12]. By receiving and saving the signatures, which were broadcasted regularly by RSUs or actively requesting signatures, vehicles obtain movement trajectories. In V2V communication, vehicle has to send information with its motion information. From this they concluded that ''Vehicles with the same or similar motion trajectories are Sybil attackers"
They focused and took assumption that, they are on an early stage VANET, when the number of smart vehicles are only a small fraction of the vehicles on the road and the only infrastructure components available are the RSUs. And even about RSU they took assumption that, they are tamper proof devices, storing secure information and gathering either certified random key pairs or certified timestamps. Which is not feasible approach after one certain extent. Their simulation shows that it works with a small flake positive rate in simple roadway architecture, which cannot be the case everywhere. Because if these kind of approach there comes limitations like in a traffic congested situation , vehicles move very slowly so they could receive similar timestamp certificates from the same RSUs located around the congested area. And it cannot be applied in a straightforward way to an urban environment with a complex road infrastructures and huge amount of vehicles

C. Similarity of neighboring info

Grover et al[13] defined this method to detect Sybil attack by exchanging and computing neighboring information between different vehicles. If some nodes observe that they have similar neighbors for a significant duration of time, these similar neighbors are defined as Sybil nodes. It doesn't having the role of RSU for detection.

V. SYSTEM EVALUTION

Prior EBRS was having one hidden loophole, which has been sorted by this proposed EBRS method. In that scenario if one entering RSU point has been identified by attacker, than it is easier to perform intrusion in system because of that MAJOR ASSUMPTION that RSU and TA has been secured. This hypothesis leads to system vulnerability that is, if just malicious node take entry from the initial RSU, this would get reputation value increment by the time as per previous work mechanism of reputation system. So by certain time period completion even this illegitimate node's would have increased reputation value and counted as legitimate node, as authentication mechanism would not recognize this malicious activity at an entry point. It is like door is open for everyone, and they are saying, all those who are coming from this gate is trusted. This major vulnerability has been eliminated by this proposed system by the use of hash based activity logs.

Table- I: Name of the Table that justify the values

Detection Methods	Sybil attack with fabricated identities	Sybil attack with stolen identities	Conspired Sybil attack	Message integrity	Privacy prevention	RSU security Assumptions	Feasibility on every road traffic conditions	Capability to run in various traffic environment
RSSI[11]	-	-	×	N/A	N/A			
TSA[12]	-	-	N/A	✓	×	✓	×	Only on simple roadway architecture
SNI[13]	-	-	N/A	N/A	×	N/A		
EBRS[9]	✓	✓	✓	✓	✓	✓	✓	
Enhanced EBRS	✓	✓	✓	✓	✓	×	✓	

Instead of relying on reputation values we are considering attached hash values, which is even helping to reduce complexity of design, it is simpler than reputation value mechanism.

VI. SIMULATION

Simulation has been done with latest renowned framework for VANET research, which is known VEINS, it is based on two well established simulators, one is OMNeT++, which is event based network simulator[14], and another one is SUMO[15], which is a road traffic simulator. Veins framework[16] is working as a bridge to perform symmetric simulations to get results of network and road traffic both by these two simulators, SUMO and OMNeT++.

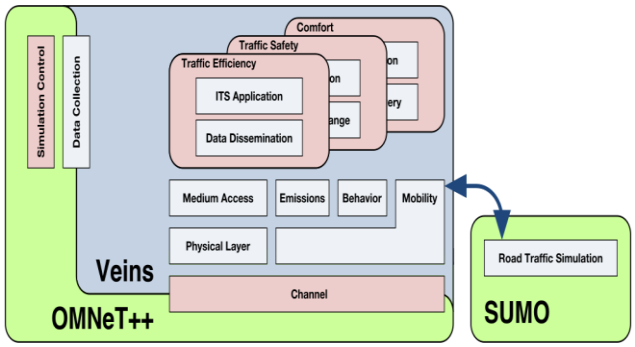

Figure 5 Veins Architecture[17]

Table II Result with experimental scenarios

Sr. No.	Scenario Name	No. of cars Enrolled through 1st Initial RSU	Cars Count traced at 2nd RSU	Cars Count traced at 3rd RSU	Distance Between RSUs	Detection of Sybil Node(Location)	Distance traversed by Sybil Node
1	Regular Scenario	17	17	17	5km	N/A	N/A
2	Sybil attack with fabricated identity	17	17	18	5km	At RSU3	RSU2-RSU3
3	Sybil attack with Stolen identity	17	18	17	5km	At RSU2	RSU1-RSU2
4	Conspired Sybil attack	17	20	17	5km	At RSU2	RSU1-RSU2

VII. RESULT ANALYSIS

1. Regular Scenario: -

In this scenario 17 cars has been registered at initial RSU and traversing in the VANET environment. These count of cars stays as it is in this scenario, it is regular scenario which has not been compromised by any Sybil attack.

2. Sybil attack with fabricated nodes. :-

Fictions nodes are considered as fabricated nodes in this scenario. The nodes which are additionally inserted by- Malicious attacker, which is not replica of any legitimate nodes moving under the VANET environment. There are 17 cars passed through initial RSU, they all are registered within the scope. In this scenario distance between two RSUs has been defined in kilometers and it is 5 km in between. At RSU3 number of count found 18, by tracing this fabricated node. And that car would not having authentic hash numbered identity. By tracing that fabricated car, it would got eliminated at RSU3. So this car has traversed between RSU2 to RSU3 only after reaching the up next RSU. It couldn't survive in our VANET environment. Here, and as a result it is eliminated from the scenario of fabricated Sybil node./

3. Sybil attack with stolen identities:-

Here stolen identities referred as a replica of legitimate car nodes. This stolen identities may mislead the traffic by using authentic person's trust credit or reputation.

There are 17 cars passed through initial RSU, they all are registered within the scope. In this scenario distance between two RSUs has been defined in kilometers and it is 5 km in between. At RSU2 number of count found 18, by tracing this Sybil node of legitimate node that car would not having authentic hash numbered identity as authentic car node. By tracing that illegitimate car, it would got eliminated at RSU2. So this car has traversed between RSU1 to RSU2 only after reaching the up next RSU. It couldn't survive in our VANET environment. Here, and as a result it is eliminated from the scenario of stolen id Sybil node.

4. Conspired Sybil attack:-

Conspired Sybil attack is defined here as a multiple stolen identities inserted at a single stroke. It is recognized as a conspired Sybil attack where there would be more than one stolen identities roaming in the VANET environment. There are 17 cars passed through initial RSU. At RSU2 number of count found 20, by tracing these conspired Sybil node. And those cars would not have authentic hash numbered identities. By tracing that illegitimate cars, it would got eliminated at RSU2, and as a result they're eliminated from the scenario of conspired Sybil attack.

VIII. CONCLUSION

By this research, prior work has been observed and their system has been extend to one step ahead to provide complete VANET security. Instead of reputation based mechanism, hash based mechanism has been designed to Prior system was providing just Security for V2V communication, by the proposed system, along with V2V, V2I communication also taken in consideration to mitigate Sybil attack destruction.

REFERENCE

1. Y. Yang, Z. Wei, Y. Zhang, H. Lu, R. Choo, and H. Cai, "V2X Security : A Case Study of Anonymous Authentication," *Pervasive Mob. Comput.*, 2017.
2. E. C. Eze, S. Zhang, and E. Liu, "Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward," *ICAC 2014 - Proc. 20th Int. Conf. Autom. Comput. Futur. Autom. Comput. Manuf.*, no. September, pp. 176–181, 2014.
3. R. Mishra, "VANET Security : Issues , Challenges and Solutions," pp. 1050–1055, 2016.
4. M. Li *et al.*, "Security in VANETs Abstract : Table of Contents :," pp. 1–12, 2014.
5. S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular Ad Hoc network," *J. Netw. Comput. Appl.*, vol. 37, no. 1, pp. 380–392, 2014.
6. H. Kaur, "Sybil Attack in VANET," pp. 3201–3204, 2016.
7. J. R. Douceur, "The Sybil Attack," pp. 251–260, 2007.
8. U. Parmar, S. S.- Astt, and M. Prof, "Overview of Various Attacks in VANET," vol. 3, no. 3, pp. 120–125, 2015.
9. X. Feng, C. yan Li, D. xin Chen, and J. Tang, "A method for defensing against multi-source Sybil attacks in VANET," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 2, pp. 305–314, 2017.
10. B. Yu, C. Z. Xu, and B. Xiao, "Detecting Sybil attacks in VANETs," *J. Parallel Distrib. Comput.*, vol. 73, no. 6, pp. 746–756, 2013.
11. M. S. Bouassida, G. Guette, M. Shawky, and B. Ducourthial, "Sybil nodes detection based on received signal strength variations within VANET," *Int. J. Netw. Secur.*, vol. 9, no. 1, pp. 22–33, 2009.
12. G. Kambourakis, D. Damopoulos, D. Papamartzivanos, and E. Pavlidakis, "Co Co," no. January, pp. 523–538, 2014.
13. J. Grover, V. Laxmi, and M. S. Gaur, "Sybil attack detection in VANET using neighbouring vehicles," *Int. J. Secur. Networks*, vol. 9, no. 4, pp. 222–233, 2014.
14. "Getting Started - OMNeT++ Tutorials." [Online]. Available: https://docs.omnetpp.org/tutorials/tictoc/part1/. [Accessed: 07-May-2019].
15. D. Krajzewicz, "Traffic Simulation with SUMO – Simulation of Urban Mobility," 2010, pp. 269–293.
16. "Documentation - Veins." [Online]. Available: https://veins.car2x.org/documentation/. [Accessed: 11-Mar-2019].
17. "Documentation - Veins." [Online]. Available: https://veins.car2x.org/documentation/. [Accessed: 05-Jun-2019].

AUTHORS PROFILE

Kunal J. Dutt, Pursuing Master's in cyber security domain from GTU-School of Engineering & Technology, Gandhinagar, India. Finale year student performing research in the VANET Security

Seema B. Joshi, Completed M,Tech in cyber security & Incident response from Gujarat Forensic Science University, Gandhinagar. Working as Assistant professor in cyber security at GTU-School of Engineering & Technology. Having 10 years of experience in teaching. Pursuing PhD in the domain of Cloud Security. 4 papers has been published and 2 books has her contribution in it..