Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 8, August 2016, pg.230 – 240

Sybil Node Detection Using Neighbourhood Information Passing

Pinky Mittal[1], Deepti Ahlawat[2]
M.TECH Scholar & N.C.C.E, Israna, Assistant Professor & N.C.C.E, Israna
pinky.mittal231@gmail.com, deeptijaglan@gmail.com

Abstract— Everyday people spend time and undergo stress waiting in traffic jams in their vehicles. In addition, traffic accidents occur and take away the Vehicular ad hoc networks (VANETs) are one important type of the mobile ad hoc networks (MANETs) developed as the basis of ITS to provide safer, better, and more efficient roads. In VANETs, the main network nodes are the smart vehicles and the road-side infrastructure units (RSUs) that are enabled to communicate with each other through vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. Such communications provide a variety of applications ranging from exchanging life-saving information, such as environmental and driving hazards, to traffic congestion, touristic messages, and advertisements. Many methods are proposed, such as RSSI-based (Received Signal Strength Indicator) detection method, vehicle movement trajectory based methods But there are various things that make the existing methods cannot work well one is conspired Sybil attack, in which malicious vehicles obtain multiple false identities through the way of forgery, stolen and share their identities with the accomplices. It is very difficult to be defended and detected, especially when it is launched by some conspired attackers using their legitimate identities. In a Sybil attack a malicious node can produce and manipulation a colossal number of logical individualities on a solitary physical device. This gives the illusion to the web as if it were disparate legitimate nodes. A malicious device's supplementary individualities are recognized as Sybil nodes. This counselled work presents an algorithm to notice Sybil nodes possessing fabricated individualities in a vehicular ad hoc network we have worked on neighbouring nodes information based method to isolate the Sybil nodes.

Keywords— Vanet, Sybil attack, Wireless, MANET

I. INTRODUCTION

Everything is becoming wireless. The fascination of mobility, accessibility and flexibility makes wireless technologies the dominant method of transferring all sorts of information. Satellite televisions, cellular phones and wireless Internet are well-known requests of wireless technologies. This work presents an enthusing wireless request and introduces a puny contribution to its scrutiny community.Wireless scrutiny earth is producing faster than each supplementary one. It serves an expansive scope of requests below disparate topologies every single one of that comes alongside a little new enumerated protocol.

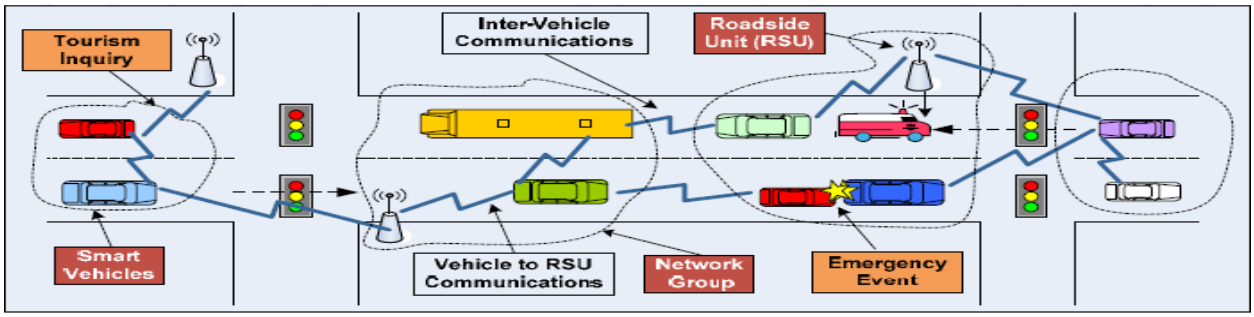


Fig. 1.1: Basic structure of VANET

VANET is the knowledge of constructing a robust Ad-Hoc web amid mobile vehicles and every single supplementary, as well, amid mobile vehicles and roadside units. Mobile Ad-Hoc Network (MANET) is a wireless knowledge whereas all nodes are one level topology and can converse undeviatingly alongside every single supplementary across a solitary hop or multi-hop lacking the demand of centralized nodes. The critical usefulness of this knowledge arises after it is needed to craft a web alongside an extremely fast placement period and after is tough to have static centralized nodes such in cases of battlefields, forests or in usual catastrophes. Factually articulating, VANET is a distinct case of the finished MANET to furnish contact amid adjacent vehicles and amid vehicles and adjacent fixed roadside equipments.

Attacks in VANET

1. Sybil Attack: Such aggressions are forging the individuality of countless vehicles that are utilized to cast each kind of attack on the arrangement and it is additionally utilized to wreck the connections of web, topologies, web transmission expenditure.

2. Message Suppression Attack: This kind of attack, attacker discriminative drops the memo packets. For the receiver a critical Data could be grasp by these packets. So, The aim of this attack is to stop insurance powers from discovering concerning the vehicular collisions.

3. Malicious Vehicle: Privacy is the most vital protection obligation of vehicular adhoc networks. To circumvent being pursued, the use of randomly changing individualities (also shouted pseudonym) is suggested. This can lead to a situation whereas a malicious vehicle M can facilely change its individuality to node N lacking being punished.

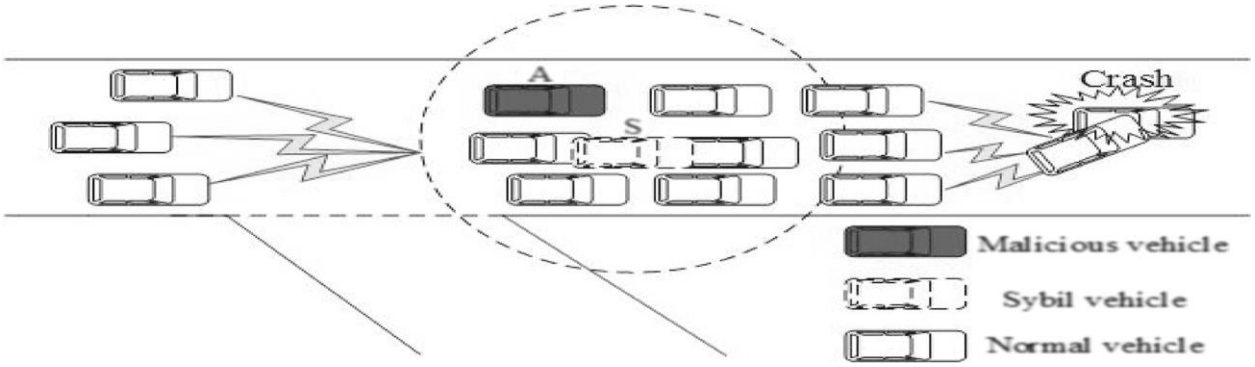


Fig. 1.2: Attack's Scenario: Sybil Attack

VANET Applications

According to the DSRC, there are above one hundred suggested requests of VANETs. These requests are of two groups, protection and non-safety related. Moreover, they can be categorized into OBU-to-OBU or OBU-to-RSU applications. Here we catalog a little of these applications.

1.Co-operative Encounter Warning: Co-operative encounter notice is an OBU-to-OBU protection request, that is, in case of each curt change in speed or steering association, the vehicle is believed atypical and shows a notice memo to alert all of the pursuing vehicles of the probable danger.

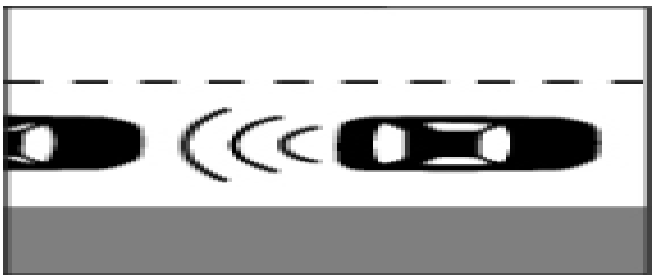


Figure 1.3: Co-operative Encounter Warning

2. Lane Change Warning: Lane-change notice is an OBU-to-OBU protection request, that is, a vehicle driver can alert supplementary vehicles of his aim to change the voyaging lane and to book an empty room in the approaching lane.

3. Intersection Encounter Warning: Intersection encounter notice is an OBU-to-RSU protection application. At intersections, a centralized node warns approaching vehicles of probable accidents and assists them ascertaining the suitable approaching speed.

4. Electronic Toll Collection (ETC): Electronic toll collection is an OBU-to-RSU non-safety application that supports the collection of payment at toll plazas using automated systems to increase the operational efficiency. Systems typically consist of OBUs that are chargeable with prepaid smart cards.

Figure 1.4: **Electronic Toll Collection (ETC)**

In the next section we will discuss about Literature which is enriched with a lot of information about Sybill Attack. A literature survey is being done to find a proper way to carry out this research. Literature review of various research papers are given below in a sequence, so that a sense can be developed according to advancement and scope in this area.

II. LITERATURE REVIEW

A brief literature review is being discussed in the following section. **Soyoung et. al.** proposed a timestamp series approach to defend against Sybil attack in a vehicular ad hoc network (VANET) based on roadside unit support. The proposed approach targets the initial deployment stage of VANET when basic roadside unit (RSU) support infrastructure is available and a small fraction of vehicles have network communication capability. Unlike previously proposed schemes that require a dedicated vehicular public key infrastructure to certify individual vehicles, in our approach RSUs are the only components issuing the certificates. **Mina, Rahbari et. al.** proposed that a vehicular communications play a substantial role in providing safety transportation by means of safety message exchange. Researchers have proposed several solutions for securing safety messages. Protocols based on a fixed key infrastructure are more efficient in implementation and maintain stronger security in comparison with dynamic structures. The purpose of this paper present a method based on a fixed key infrastructure for detection impersonation attack, in other words, Sybil attack, in the vehicular ad hoc network. This attack, puts a great impact on performance of the network. The proposed method, using an cryptography mechanism to detection Sybil attack. **Navneet et. al.** in his paper proposed that VANET is recognized as an important component of Intelligent Transportation Systems. To successfully deploy VANET, security is one of the major challenges that must be addressed. This research detects the Sybil attack a new filed is introduced in the AODV named SCID i.e. Secondary id. It maintains a unique identity of each node. Now the packet format of AODV consists sequence number as well as secondary identity i.e. SCID. **Manjunatha T. N et. al.** in the presented paper gave the general concept of wireless sensor network and security in wireless sensor network. The various existing method for the detection of Sybil attack have been discussed and an algorithm is proposed for detection of Sybil attack in wireless sensor network. By using that algorithm it will find the Sybil node or not. Current research so far focuses on the security of wireless sensor network. **Xia, Feng et.**

al. proposed an event based reputation system (EBRS), in which dynamic reputation and trusted value for each event are employed to suppress the spread of false messages. EBRS can detect Sybil attack with fabricated identities and stolen identities in the process of communication; it also defends against the conspired Sybil attack since each event has a unique reputation value and trusted value.

III. Proposed Work

Here, a way is utilized to localize the fake individualities by analysing the consistent similarity in area information. In this work, the new scheme had been counselled that will be established on to notice malicious nodes from the web that are accountable to trigger Sybil attack in the web.

Assumptions

These assumptions are:

- The speed of the mobile nodes are fixed on the defined roads
- The RSUs are responsible to maintain the information about all vehicles.
- The mobile nodes have to present its neighbor node information to RSUs.
- The RSUs can maintain the neighbor node information about all the nodes.

Detection and Isolation Algorithm

Various Inputs of the Algorithm are:

- Let N be an elected Node in the network(cars).
- Let SV[N] be the Speed of Node N.
- Let NV[N] be the neighbor vehicles of node N.
- Determine the TV[N] be the Threshold Value.
- Let R be an RSU.
- Let n be the Number of new Node, malicious Node (car).

Various Outputs of the Algorithm are:

- Detection of Malicious Node (car).

Various Assumptions are:

- RSU have complete data of each vehicle calculation performed at RSU server. For any change hello packet is transmitted.

Algorithm 1: Detection & Isolation Algorithm

Step 1: Registration Process Start.

Step 2: N Communication with ”Hello Packets” withR.

Step 3: if INFO[Credentials]==INFO[R] then

RSU assign Identification No[N_i] to N.

else

Repeat Step 1;

end if

Step 4: if INFO[N_i]= =INFO[N] **then**

if SV[Ni]=TV[N_i] **then**

Node is detected as Malicious Node.

else

Node is detected as Legimitimate Node & Communication begins between cars.

end if

end if

Step 5: RSU stores Info[NV[N_i]] to R

Step 6: if new Node Enters in Networ k **then**RSU Verify Gathering Information of NV of new Node.

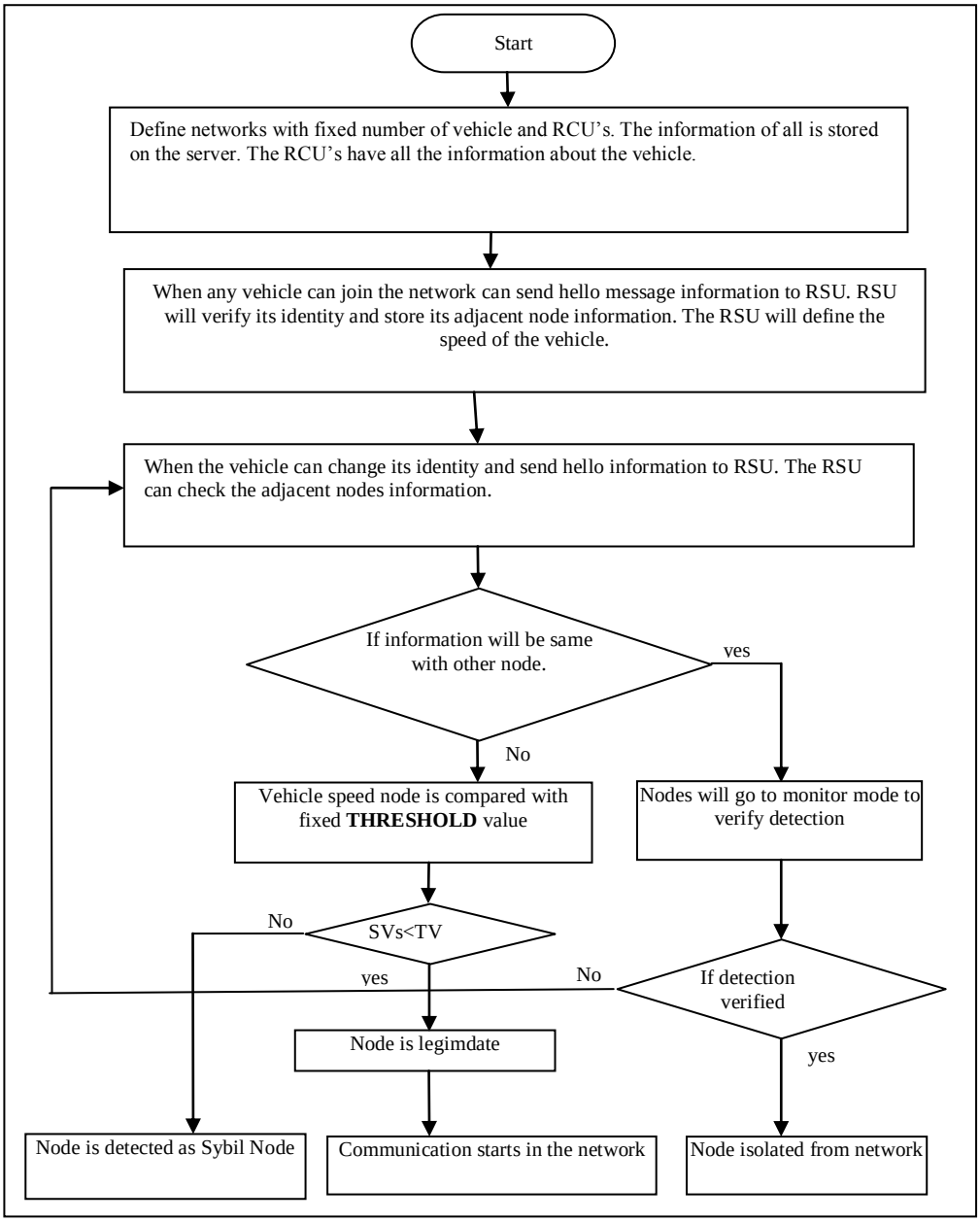
end if

Step 7: ifINFO[n[NV]==INFO[R[NV]] **then** no Malicious Detected else Monitoring=True

end if

Step 8: ifMalicious car == detected**then**Isolate Malicious Car with IDelse Repeat Step 8;

end if



Considered NS2 (Network Simulator - 2), due to the expansive collection of functional models for Simulations. The Web Simulator edition 2.34 is utilized, alongside the configured span of 1000m X 1000m. A little nodes are configured to deed as RSU's and supplementary are configured as vehicles. In finished 18 nodes are utilized for this simulation purposes. RSU nodes are fixed nodes whereas the supplementary nodes are advancing at speed of 30m/s. For the detection of malicious nodes, we configured 2 nodes to deed as malicious nodes. AODV protocol is utilized for contact alongside 512 kilobytes packet size and TCP packet Types.

Table 4.1 summarize all the parameters values which are considered for the system.

Simulator	NS-2.35
Area	1000m X 1000m
Number of Nodes	18
Vehicle Speed	30m/s
Routing protocols	AODV
Packet Size	512kb
Threshold Value	60m/s
Packet Type	TCP
Movement Model	Random Way Point

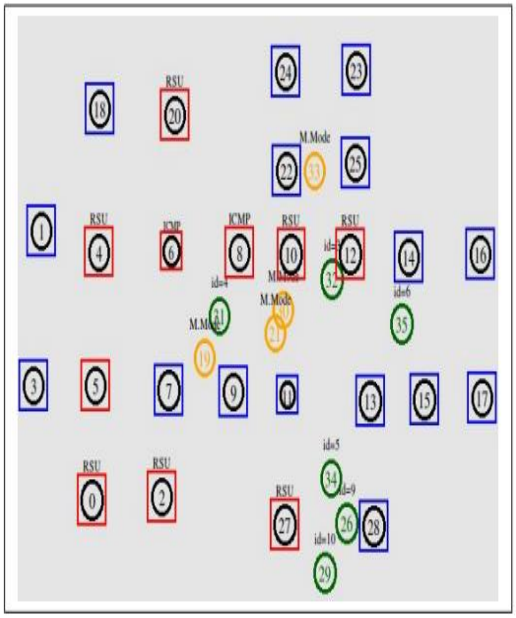


Fig.4.1.:Monitoring Process of Malicious Nodes

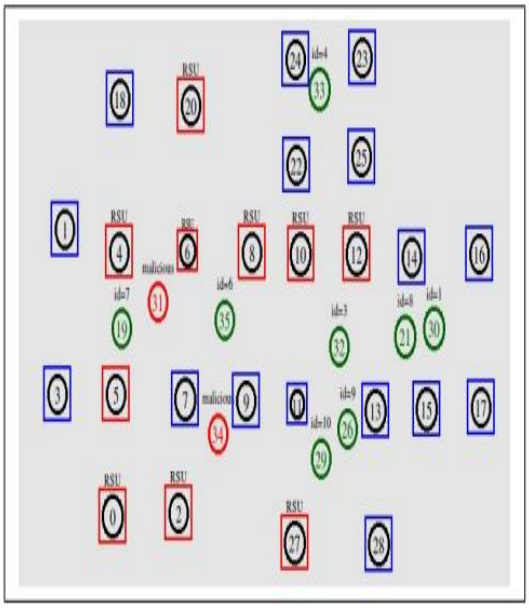


Fig.4.2:Detection of Malicious Nodes

Figure 4.3: shows the comparison of Event Based Reputation System approach of Sybil node detection with the proposed method Neighbourhood Based (NHB) in terms of routing delay.

Figure4.4: shows the comparison of Event Based Reputation System approach of Sybil node detection with the proposed method Neighbourhood Based (NHB) in terms of collision avoidance.

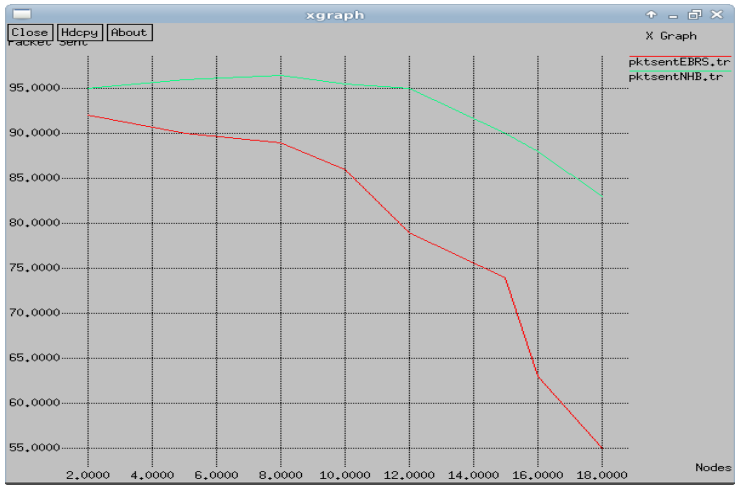


FIGURE4.5: SHOWS THE COMPARISON OF EVENT BASED REPUTATION SYSTEM APPROACH OF SYBIL NODE DETECTION WITH THE PROPOSED METHOD NEIGHBOURHOOD BASED (NHB) IN TERMS OF PACKET SENT.

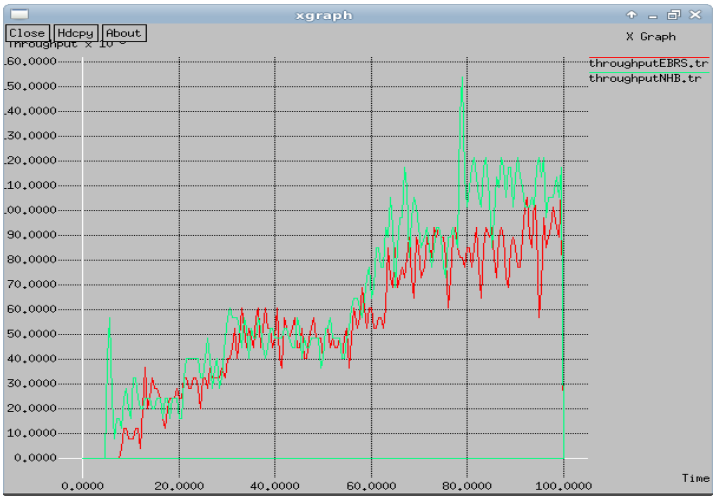


Figure4.6: shows the comparison of Event Based Reputation System approach of Sybil node detection with the proposed method Neighbourhood Based (NHB) in terms of throughput.

IV. CONCLUSIONS

In VANET, countless aggressions are being activated by the malicious nodes. So using the proposed method, we came to the following conclusions: Sybil attacks can be avoided upto more extent and communication becomes much more reliable if nodes can communicate directly with each other which has been done in the proposed method. Results indicate that the proposed method generates less amount of delay as compared to other methods. Also the throughput, collision avoidance and number of packets sent in the proposed method are also achieved better.

Acknowledgement

I express my sincere and deep gratitude to Mr. Jagtar Singh Assistant Professor and H.O.D of ECE department, Ms. Deepti Ahlawat Assistant Professor of ECE department, N.C.College of Engineering, Israna (Panipat) for her guidance, valuable suggestions, immense help, encouragement and friendly behaviour throughout the investigation in the dissertation.

I cannot conclude this acknowledgement without mentioning my parents. It would not be possible for me to complete this project work without their love, encouragement and support.

REFERENCES

[1]. Bin, Xiao, Bo Yu, and Chuanshan Gao. "Detection and localization of sybil nodes in VANETs." In Proceedings ACM workshop on Dependability issues in wireless ad hoc networks and sensor networks, pp. 1-8, 2006.

[2]. Gilles, Guette, and Bertrand Ducourthial. "On the sybil attack detection in vanet." In Mobile Adhoc and Sensor Systems ,MASS ,IEEE International Conference on, pp. 1-6, 2007.

[3]. Tong, Zhou, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty. "Privacy-preserving detection of sybil attacks in vehicular ad hoc networks." In Mobile and Ubiquitous Systems: Networking & Services, MobiQuitous, IEEE. Fourth Annual International Conference on, pp. 1-8, 2007.

[4]. Gongjun, Yan, Stephan Olariu, and Michele C. Weigle. "Providing VANET security through active position detection." Computer Communications vol. no. 12 ,pp 2883-2897, 2008.

[5]. 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 Military Communications Conference, MILCOM IEEE, pp. 1-7, 2009.

[6]. Mohamed Salah, Bouassida, Gilles Guette, Mohamed Shawky, and Bertrand Ducourthial. "Sybil Nodes Detection Based on Received Signal Strength Variations within VANET." IJ Network Security, vol. no. 1,pp. 22-33, 2009.

[7]. Sohail, Abbas, Madjid Merabti, and David Llewellyn-Jones. "Signal strength based Sybil attack detection in wireless Ad Hoc networks." In Developments in eSystems Engineering (DESE), IEEE Second International Conference on, pp. 190-195, 2009.

[8]. Subir, Biswas, Md. Mahbubul Haque, and Jelena V. Misic. "Privacy and Anonymity in VANETs: A Contemporary Study." Ad Hoc & Sensor Wireless Networks, vol. no. 2-3 , pp.177-192, 2010.

[9]. Al-Qutayri, Mahmoud, Chan Yeun, and Faisal Al-Hawi.m "Security and privacy of intelligent VANETS". INTECH Open Access Publishers, 2010.

[10]. Mina, Rahbari, and Mohammad Ali Jabreil Jamali. "Efficient detection of sybil attack based on cryptography in VANET." 2011.

[11]. Irshad Ahmed, Sumra, Iftikhar Ahmad, Halabi Hasbullah, and Jamalul-lail Bin Ab Manan. "Classes of attacks in VANET." In Electronics, Communications and Photonics Conference (SIECPC), Saudi International,IEEE, pp. 1-5, 2011.

[12]. Nicole, El Zoghby, Véronique Cherfaoui, Bertrand Ducourthial, and Thierry Denoeux. "Distributed Data fusion for detecting Sybil attacks in VANETs." In Belief Functions: Theory and Applications, Springer Berlin Heidelberg, pp. 351-358, 2012.

[13]. Rasheed, Hussain, Sangjin Kim, and Heekuck Oh. "Privacy-aware VANET security: Putting data-centric misbehavior and sybil attack detection schemes into practice." In Information Security Applications, Springer Berlin Heidelberg, pp. 296-311, 2012..

[14]. Adil Mudasir, Malla, and Ravi Kant Sahu. "Security attacks with an effective solution for DoS attacks in VANET." International Journal of Computer Applications vol. no. 22, 2013.

[15]. Navneet, Rakesh Gill "Sybil Attack Detection and Prevention Using AODV in VANET", International Journal of Computer Science and Management Studies vol. no. 13, 2013.

[16]. Manjunatha T. N, Sushma M. D, Shivakumar K. M "Security concepts and Sybil attack detection in wireless sensor networks" in International Journal of Emerging and Technology in Computer Science(IJETTCS), 2013.

