ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

ICMP and Monitoring to Detect and Isolate Sybil Attack in VANET

Jaydeep P. Kateshiya[1], Anup Parkash Singh[2]

P.G. Student, Department of Computer Engineering, Lovely Professional University, Punjab, India[1]

Assistant Professor, Department of Computer Engineering, Lovely Professional University, Punjab, India[2]

ABSTRACT: MANET stands for Mobile Ad hoc Network. It is a robust infrastructure less wireless network. Malicious vehicles can degrade the network performance by triggering some security attack. VANET are self-configuring networks composed of a collection of vehicles and elements of roadside structure linked with each other without requiring any infrastructure, sending and receiving information of current traffic situation. These are used for the communication among the mobile vehicles.It has some security issues like attacks, authentication etc. In this work, a novel technique has been proposed to detect malicious vehicles and isolate Sybil attack from the network. This will help to improve network performance.

KEYWORDS: MANET, VANET, Malicious node, Sybil Attack. Collision, V2V communication.

I. INTRODUCTION

MANET stands for Mobile Ad hoc Network. It is a robust infrastructure less wireless network. It can be formed either by mobile nodes or by both fixed and mobile nodes. Nodes are randomly connected with each other and forming arbitrary topology. They can act as both routers and hosts. Their ability to self-configure makes this technology suitable for provisioning communication, for example disaster-hit areas where there is no communication infrastructure or in emergency search. In MANET routing protocols for both static and dynamic topology are used. An ad hoc network is a wireless network describe by the nonexistence of a centralized and fixed infrastructure. The absence of an infrastructure in ad hoc networks poses great challenges in the functionality of these networks [1]. VANET's is a subset of MANET and best example of VANET is Bus System of any university which is connected together. These buses are moving in different parts of city to pick or drop students if they are connected together, make an Ad hoc Network [2]. One of the most capable areas of research is the study of the communications among vehicles called Vehicular Ad-hoc Networks (VANETs). This kind of networks are self-configuring networks composed of a collection of vehicles and elements of roadside structure linked with each other without requiring any infrastructure, sending and receiving information of current traffic situation [3]. These are used for the communication among the mobile vehicles. The communication being carries on even if the vehicles are moving in the different direction with in a particular area. Intelligent vehicular ad hoc networks are used in case like collision of the vehicles or any other types of mobility problems [4]. It is uses the scheme intelligently and the flow less communications goes on. Vehicular adhoc network are wireless networks where all the vehicles from the nodes of the network. It is for the driver comfort and road safety, the inter-vehicle communication provide them. Vehicular ad-hoc network is subclass of mobile ad hoc networks which provides a distinguished approach for intelligent transport system [5]. It is very necessary for all the vehicles. Vehicular ad hoc network is special form of MANET which is vehicle to vehicle roadside wireless communication network. It is autonomous and self-organizing wireless communication network, where all the nodes in VANET involve themselves as servers or client for exchanging and sharing information.

1.1 Major Issues in VANET: There are some issues in VANET. These are as follow:

1. High Mobility: Due to high mobility all the nodes are not interacted properly with each other because they have to learn about others behaviour first according to learn based scheme. It also decreases efficiency of the system [10].
2. Real-time Guarantee: VANET applications are used for hazard warning, collision avoidance, and accident warning information, so applications involve strict deadlines for proper message delivery [8].

3. Privacy and Authentication: It is required to follow the vehicles for the identification of vehicles from the message they send for authentication of all message transmission, which most consumers will not like others to know about their personal identification. Therefore a system wants to be introduced which enables message to be unknown to the common nodes but also recognition by central authorities in cases like accidents.

4. Location Awareness: For the proper location awareness GPS system is required to handle the VANET application. If there is no Proper system for location identification, delay is there automatically.

5. Delay in VANET: In a VANET delay issue should be minimum for the new path identification. In this system vehicle and RSU detect chances of collision between multiple vehicles are not able to communicates amongst themselves. The system will collect data about vehicles that are coming in opposite direction and are approaching towards the destination. For this, there are many safety applications are present in VANET to decrease the road accident and loss of life of the occupants of vehicles. Collision leads the jam problem. To overcome this problem delay should be minimum.

1.2 Attacks in VANET:

1. Denial of Service Attack: In DOS attack the main objective is to prevent legitimate user from accessing resources and services. This attack can be trigger by jamming the whole channel and network so that no authorized vehicle can access the network. It is serious problem in which user is unable to communicate with the user due to DOS attack. At the basic level, attacker forces node and make it busy to do unnecessary tasks by overwhelming it so that it could not do necessary tasks. So it is responsible for packet dropping [7].

2. Distributed Denial of Service Attack: DDOS is more harmful than DOS attack because it is in distributed manner. Different types of locations are used by the attacker to launch the attack. It might be possible that they use different time slots for sending messages. The nature of the message and time slot varied from vehicle to vehicle. DDOS is possible at V2V and V2 I. Its main objective is to slow down the network and jam the network [7].

3. GPS Spoofing: Table is maintained in the network to update all the information regarding identify of the vehicle and geographic location of the vehicle. Attacker generate GPS satellite signal to fool vehicle which are more effective than the original signals.

4. Timing Attack: There should be accuracy in the time for the best performance of the network so delay should be less in any application. Timing attack is an issue in ITS safety application. In this attack, attacker instead of modify the data; add more content in the original data. Due to addition message takes more slot to reach to the destination rather than required time. So ITS application is crucial application which is dependent on time and it requires data transmission on time otherwise serious accident may happen as shown in figure 1 [7].

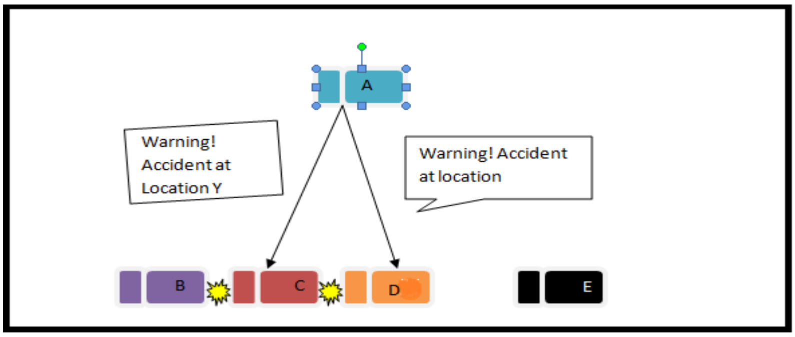
A
Warning! Accident at Location Y
Warning! Accident at location
B
C
D
E

Fig.1: Timing Attack

II. BACKGROUND AND RELATED WORK

In paper [1], they present a lightweight security scheme for detecting and localizing Sybil nodes in VANETs, based on statistic analysis of signal strength distribution. Their scheme is a distributed and localized approach, in which each vehicle on a road can perform the detection of potential Sybil vehicles nearby by verifying their claimed positions. They first introduce a basic signal-strength-based position verification scheme. In this technique, traffic patterns and support from roadside base stations are used to their advantage then, propose two statistic algorithms to enhance the accuracy of position verification. The statistic nature of our algorithms significantly reduces the verification error rate.InGPS and RSSI signal measurements are used for detecting Sybil nodes. The proposed scheme uses Vehicle-to-Vehicle (V2V) communications to confirm reported positions of vehicles by referencing the RSSI measurements. To correct inaccuracies arising from RSSI measurement, caused by vehicle mobility, traffic patterns and support from roadside base stations are used.

In paper [2], they propose a security protocol to detect Sybil attacks for position based applications in privacy preserved vehicular ad hoc networks (VANETs). Vehicles in our protocol identify Sybil attacks locally in a cooperative way by examining the rationality of vehicles' positions to their own neighbours. The attack detection utilizes the characteristics of communication and vehicles' GPS positions which are included in the periodically broadcasted safety related messages. No extra hardware and little communication and computation overhead will be introduced to vehicles. Therefore, their protocol is very light weighted and suitable for real applications. Moreover, a smart attacker scenario in which a malicious vehicle may adjust its communication range to avoid detection and the malicious vehicles' collusion scenario are also considered. Simulation results based on NS2 are presented to demonstrate the performance of the proposed protocol.

In paper [3] proposed a lightweight and scalable protocol called Privacy Preserving Detection of Abuses of Pseudonyms protocol to detect Sybil attacks in VANET. In this protocol, a malicious user pretending to be multiple (other) vehicles can be detected in a distributed manner through passive overhearing by s set of fixed nodes called road-side boxes (RSBs). The detection of Sybil attacks in this manner does not require any vehicle in the network to disclose its identity; hence privacy is preserved at all times. He results also quantify the inherent trade-off between securities, i.e., the detection of Sybil attacks and detection latency, and the privacy provided to the vehicles in the network. From the results, we see our scheme being able to detect Sybil attacks at low overhead and delay, while preserving privacy of vehicles. Using this protocol, the multiple vehicles which are affected by malicious user can be detected in a distributed manner through passive listener using set of fixed nodes called road-side boxes (RSBs). The detection of Sybil attacks in this manner does not require any vehicle in the network to explore its identity; hence privacy is preserved at times.
In [4] represents a paper based on routing protocols called RBVT, road based using vehicular traffic information routing which is based on the existing routing protocol in city based vehicular ad-hoc networks (VANETs). RBVT protocols leverage real time traffic information to create road based paths consisting of successions of road intersection and high probability, network connectivity among all the systems. In this paper use the geographical forwarding is used to send the packets between intersection paths, reducing the sensitivity within the paths to individual node movements. In the dense network high contention and optimize the forwarding using a distributed receiver based election of next hops, it is based on the multi-criteria prioritization function taking into account non-uniform radio propagation. This paper designs the reactive protocol RBVT-R and proactive protocol RBVT-P and compared them against MANETs protocols like AODV, OLSR, GPRS. Other protocol representative is like VANET. In the simulation result shows that in the urban settings shows that RBVT-R protocol best in term of delivery rate, with up to 40% increase compared to some existing protocols. In the protocol terms of average delay, RBVT-P performs best and 85% decreased as compared to other protocols.

III. SYBIL ATTACK IN VANET

It consists of sending multiple messages from one node with multiple identities. Sybil attack is always possible except the extreme conditions and assumptions of the possibility of resource parity and coordination among entities. When any node creates multiple copies of itself then it creates confusion in the network. Claim all the illegal and fake ID’s and Authority [6]. It can create collision in the network. This type of situation is known as Sybil attack in the network. This system can attack both internally and externally in which external attacks can be restricted by authentication but not internal attacks. As there is one to one mapping between identity and entity in the network.

DOI: 10.15680/IJIRSET.2015.0405056

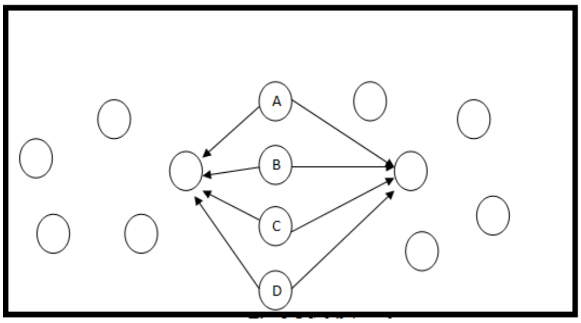

Fig.2: Sybil Attack

In figure 2, A, B, C, D nodes are Sybil nodes which create fake or similar identity in the network and collapse the network. Sybil attack is a critical attack. In this type of attack attackers generate multiple messages from different ids to other vehicles [11]. Other vehicles are thinking in this way that messages are coming from different vehicles with different ids, so there is condition of jam occurs. In this way attacker produce illusion of other vehicle and force them to choose another path and leave the road for the benefit of the attacker. Overall it is concluded that Sybil attack is performed or launched by sending multiple messages from different ids. In fig. 1.6 red colours cars have same id that is A which are responsible for trigger Sybil attack in the network. It is of two types delay sensitive and throughput sensitive.

IV. PROPOSED DESIGN

The VANET is the self-configuring type of network, in which the vehicles can move freely in the network. In such type of network, there are more chances that malicious vehicles can join the network and trigger some type of attack. Among the possible attacks Sybil attack is the most harmful attack which is possible in the network. This attack will reduce the network performance. In this work, we will work on to detect malicious vehicles in the network which is responsible to trigger such type of attacks. In this work, the new scheme has been proposed which will be based on to detect malicious nodes from the network which are responsible to trigger Sybil attack in the network [12]. The Sybil attack can harm the network throughput and delay. The throughput of the network can be reduced because network resources get wasted. The delay can be raised because packets are routed to wrong destination or long paths get followed. In this work the techniques which will be proposed are based on some assumptions. These assumptions are:

1. The speed of the mobile nodes are fixed on the defined roads
2. The RSU's are responsible to maintain the information about all vehicles
3. The mobile nodes have to present its neighbour node information to RSU's
4. The RSU's can maintain the neighbour node information about all the nodes

The malicious vehicles can change its identity every time and send hello messages to RSU's for network join. The vehicles which are on the network can register itself with the server, In the registered information the unique vehicle number and its identification number will be defined. This registered information can be available on all RSU's. When any join the network, is have to send hello message to RSU and then RSU ask nodes for their identification number. When the identification number will be successfully verified the RSU gather all the information about neighbouring or adjacent nodes of the registered nodes. The RSU will also define the speed limit of the vehicle on the road for which it is registered. When any malicious node will can its identity can send hello message to RSU, the RSU will register the malicious node but when RSU checks the adjacent node and that are different from the legitimate node. The malicious node can be detected from the network. To verify the detection process, the RSU's will flood the monitor mode messages in the network , and adjacent nodes of the malicious nodes can start monitoring the malicious nodes and detect that it is the malicious nodes. It has been simulated at NS2.

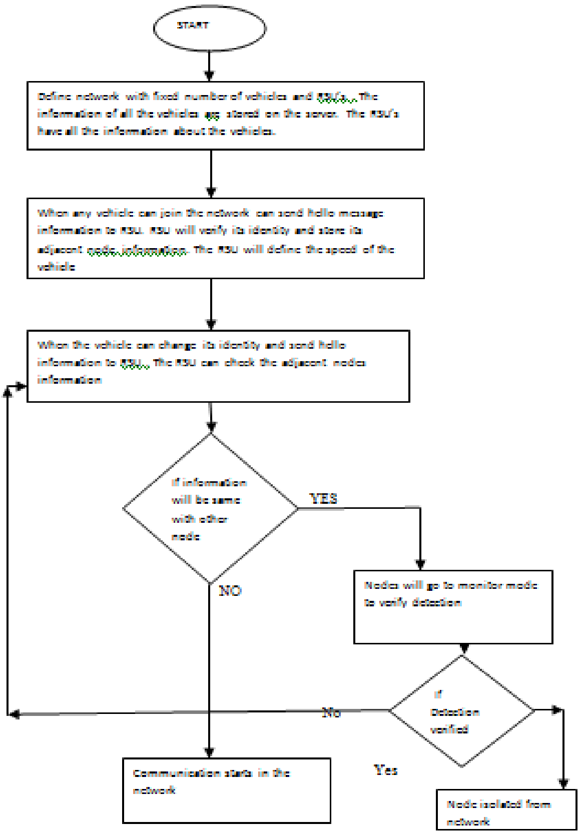
START
Define network with fixed number of vehicles and RSU's. The information of all the vehicles are stored on the server. The RSU's have all the information about the vehicles.
When any vehicle can join the network can send hello message information to RSU. RSU will verify its identity and store its adjacent node information. The RSU will define the speed of the vehicle
When the vehicle can change its identity and send hello information to RSU. The RSU can check the adjacent nodes information
If information will be same with other node
YES
NO
Nodes will go to monitor mode to verify detection
If Detection verified
No
Yes
Communication starts in the network
Node isolated from network

Fig.3:Flowchart of proposed methodology

V. PERFORMANCE EVALUATION

1. Simulation Configuration:

Our Simulation is conducted within the network Simulator (NS) 2.35 environment on platform with GCC 4.3.4 and Ubuntu 14.04.1. In NS 2.35. We make configuration with 32 nodes and flat grid size of 800x800m.

Simulation is being done byAODV routing. We generate the result in NS-2 with use of reference node technique. The graphs are used to signify the variation in throughput and end-to-end delay using the proposed method. Red line characterizes the change in case of the new scenario and green colour represents the conventional method. These two parameters are a widely used for validating the confirming the use of particular methods. Throughput can be defined as the number of packet data received per unit time whereas end-to-end delay defined as the time taken between sending of a packet and it's receiving on the destination.

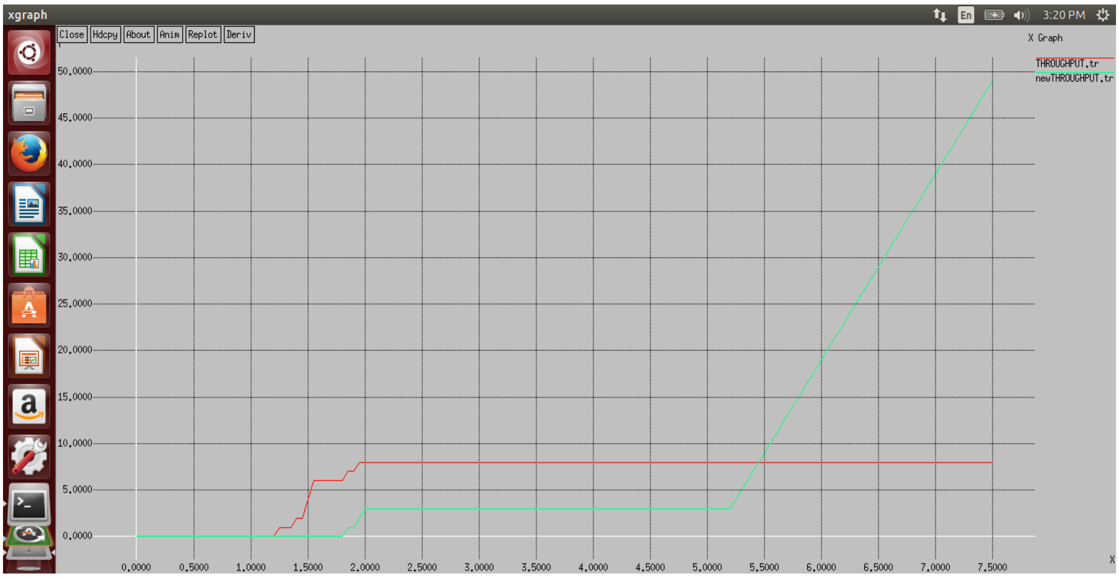

Fig. 4: Average Throughput

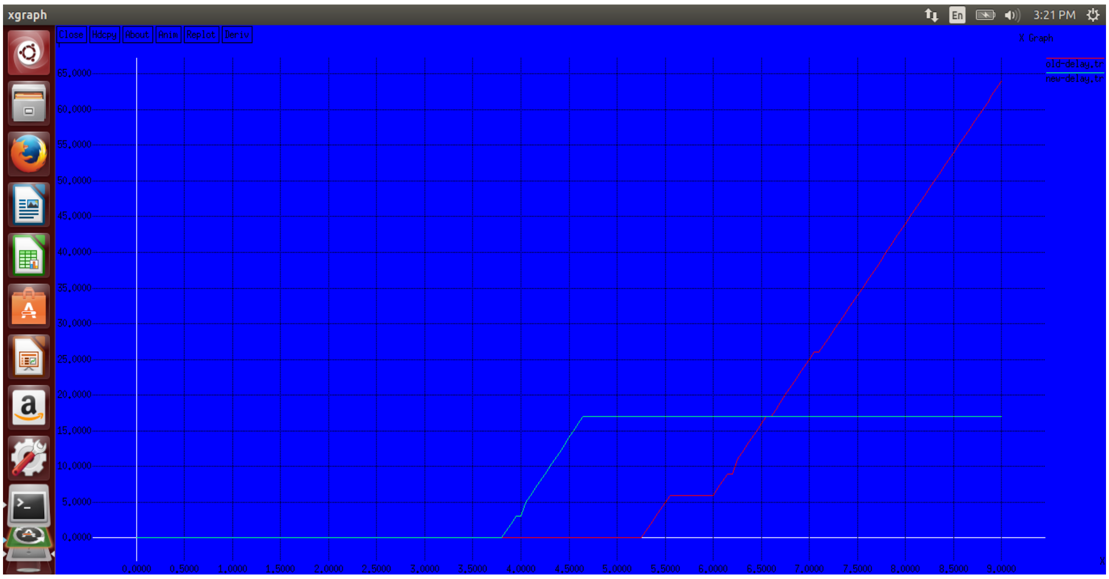

Fig 5: Average Delay

As we have applied the ICMP and monitoring node for setting up to detect malicious node in the network. So after detect the malicious node packet loss is less as compared to the previous scenario. We make the channel secure so final result comes is maximization of throughput and minimization of packet loss. In figure 6, we see that the red line is continuously increase because of dropping of the packet and green line constant after some time because of securing of channel.

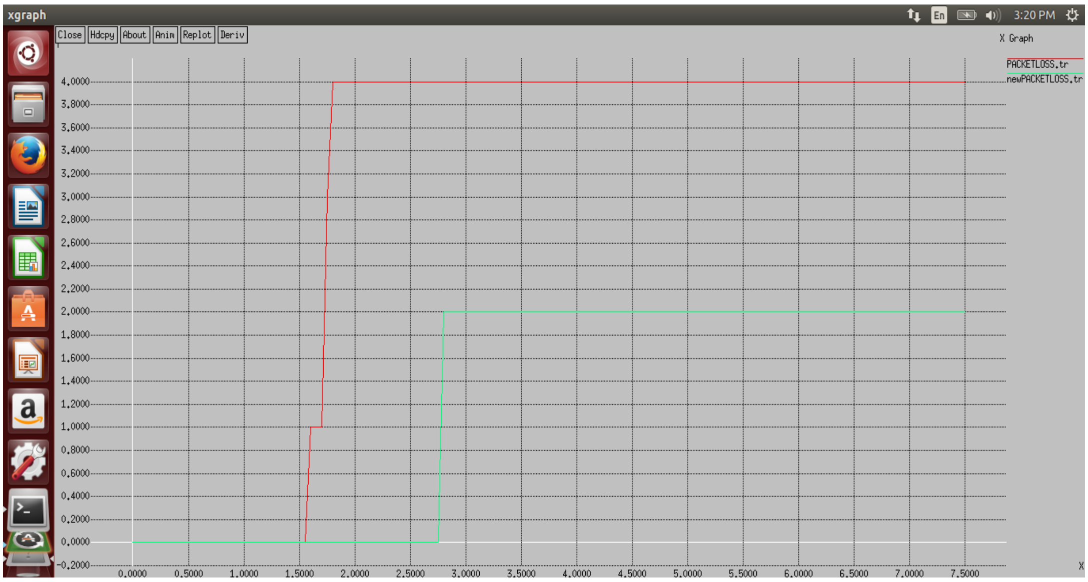

Fig. 6: Average Packet loss

Fuel emission basically how much fuel is emitted or use in vehicle. As shown above figure when malicious vehicle is present that time fuel emission are more because of every time changing id and send for communication which shown by red line. After Detect malicious vehicle using proposed method fuel emission are decrease as shown with green line.

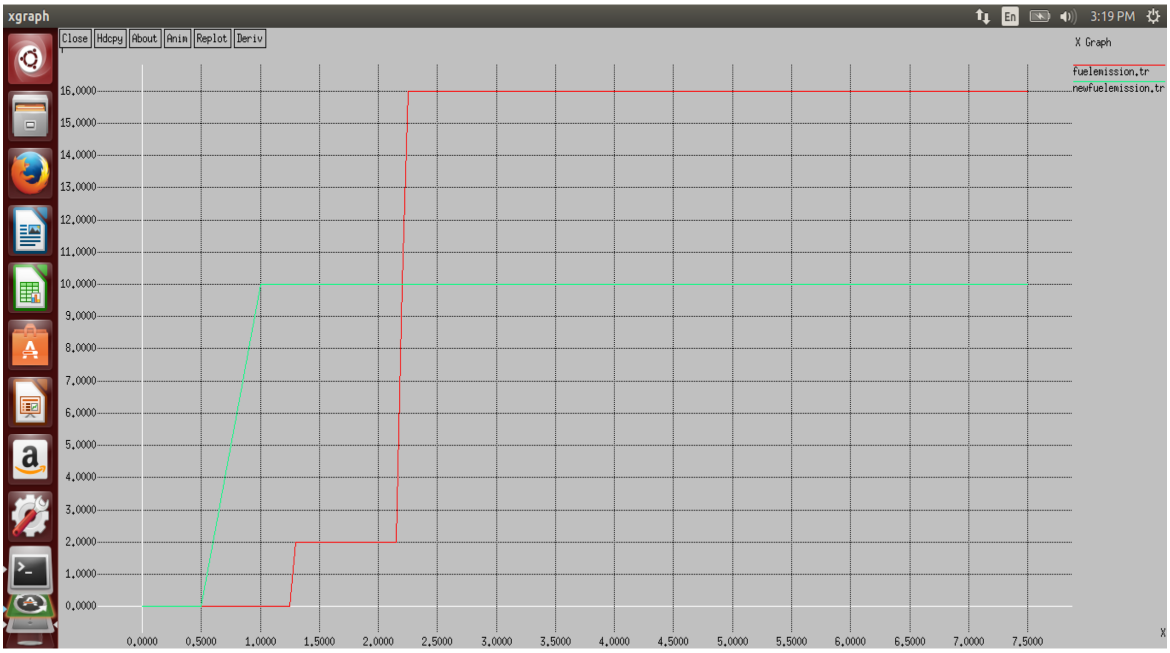

Fig. 7: Fuel Emission

VI. CONCLUSION

In VANET many attacks has been trigger by the malicious node. Therefore keeping in view above challenges there is a need to improve the efficiency of VCWC protocol so that it may be able to control both, the factors which make wireless communication unreliable and also support the above application challenges to a large extent. All the problems discussed in this paper can be raised if some of the wrong information can be flooding in the network. The wrong information can be flooding in the network by malicious vehicles. These malicious vehicles can degrade the network performance by triggering some security attack. In this work, a novel technique has been proposed to detect malicious vehicles and isolate Sybil attack from the network. This will help to improve network performance.

REFERENCES

[1] Jeong-Ah Jang "A Fixed Sensor-Based Intersection Collision Warning System in Vulnerable Line-of-Sight and/or Traffic-Violation-Prone Environment", IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, pp 1-11, 2011.

[2] Maxim and jean-Pierre Hubaux "The security of vehicular ad hoc networks",ACM,2005.

[3] SumaiyaIqbal"Vehicular Communication: Protocol Design, Testbed Implementation and Performance Analysis", IWCMC'09, June 21-24, Leipzig, Germany, pp 410-415, 2009.

[4] A. AHMAD "Hybrid Multi-Channel Multi-hop MAC in VANETs ", MoMM2010, 8–10 November, Paris, France, pp 353-357, 2010.

[5] Raya M. and HubauxJ. ,"Security of Ad Hoc and Sensor Networks", SASN '05 Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks,2005.

[6] Isaac J.T., Zeadally S., Camara J.S. (2010) IETcommunica-tionvol. 4, Iss 7, pp.894-903.

[7] Ajay Rawat, Santosh Sharma, Rama Sushil, "VANET: Security Attack and its Possible Solutions", Journal of Information and Operations Management ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, pp-301-304, 2013.

[8] AdilMudasir Mala and Ravi kantsahu, "Security Attack with an Effective Solution for DOS attack in VANET", International Journal of Computer Applications (0975 – 8887),Volume 66– No.22, March 2013.

[9] M. Raya, J. Pierre, Hubaux,"Securing vehicular ad hoc Networks" Journal of Computer Security,vol.15, pp: 39-68,jan 2007.

[10] Bilal Mustafa Umar Waqas Raja School of Computing Blekinge Institute of Technology Box 520 SE – 372 25 Ronneby Sweden," Issues of Routing in VANET",2010.

[11] Jason J. Haas and Yih-Chun Hu University of Illinois at Urbana-Champaign Urbana, Illinois, U.S.A," Real-World VANET Security Protocol Performance" , p1-7,2007.

[12] JosianeNzouonta, NeerajRajgure, Guiling Wang, Member, IEEE, and CristianBorcea, Member IEEE," VANET Routing on City Roads using Real-Time Vehicular Traffic Information" ,p1-18,2008.

DOI: 10.15680/IJIRSET.2015.0405056