Improved Multiple Malicious Node Detection Algorithm for Detecting DoS attacks in VANETs

Sushil Kumar[1], Dr. Kulwinder Singh Mann[2]
[1]*Research Scholar, IKG Punjab Technical University, Kapurthala, Punjab, India*
[2]*Professor, Guru Nanak Dev Engineering College, Ludhiana, Punjab, India*

***Abstract*—**Vehicular Adhoc Network (VANET) is specialized form of MANET in which safety is the major concern as critical information related to driver's safety and assistance need to be disseminated between the vehicle nodes. For increasing the security of nodes, the network should be available all the time. The availability of the network is hindered by the Denial of Service Attacks (DoS). In this paper, a packet detection algorithm based on frequency and velocity of the nodes is proposed. This algorithm will be able to detect the multiple malicious nodes in the network which are sending irrelevant packets to jam the network and that will eventually stop the network to send the safety messages. The proposed algorithm was simulated in NS-2 and the quantitative values of packet delivery ratio, packet loss ratio, network throughput proves that the proposed algorithm enhance the security of the network by detecting the DoS attack well in time.

Keywords *– VANETs; DoS attacks; Packet detection; malicious nodes; irrelevant data*

I. INTRODUCTION

A Vehicular Adhoc Network (VANET) is remarkable achievement towards road safety with various state-of-art safety applications. A VANET is self organized network which enable V2V and V2I communication for the exchange of important information related to road and driver safety. This network probably will play a major role for enabling comfortable traffic system on roads and will also help in avoiding unnatural traffic mishaps. VANET is a network in which communication has been done among vehicle to vehicle and vehicle to roadside unit (RSU). The short range radios are being installed in all the communicated nodes. Vehicle node has the small transmission range of 100 to 300m[6]. RSU are installed randomly depending on the categorization of the network in that specific area. RSU act in communicator between the Central Authority (CA) and vehicular node (VN)

VANET will be responsible for improved traffic safety and driver assistance[11]. In VANETs, vehicles send alert in the network regarding road conditions, collision ahead, traffic jam, weather conditions and location based services such as parking area nearby, information related to accident or incident[9].

The communication devices in the nodes will enable them to decide when to send alerts to the other nodes in the network depending upon the reliability of received data. Sometimes the received information may be useful for the vehicle and sometimes may not be and in further the received information may be useful for other vehicle depending upon the basic control decisions[9].

VANET application is categorized into two categories – Safety applications and non-safety applications. Safety applications are most critical and vital in nature as compared to non safety applications. These applications are responsible for saving human life. Non-safety applications are to make use of effective traffic control system. Non safety applications are to please passenger and driver, outdoor parking availability, directions, signals. Location map are the example of this applications. The various applications of VANETs includes comfort/entertainment (location of parking lot, hotel, petrol station etc.), safety applications (road safety information), traffic management application (road jam, collision ahead) etc [6].

The various VANET characteristics which make them unique includes high mobility, dynamic mobility, frequent disconnection, limited bandwidth, attenuations, limited transmission power, energy storage and computing.

A. Vanet Model? How It Works?

There are various entities involved in VANETs. Although the majority of nodes in VANET network are vehicles, there are some other entities which perform basic functions in these networks and they communicate and share information in many different ways. To understand the internal operation and various security issues of these networks it is customary to analyze all such entities and their relationships in the VANETs. Figure 2 shows typical VANET architecture, which contains two different environments.

a) Infrastructure Environment:- In this type of environment of the network entities can be permanently interconnected and are composed by entities which handle traffic and external services. Various entities of infrastructure environment are manufacturers, legal authority, (Trusted third party)TTP, service provider, manufacturing process uniquely

identify each vehicle. Legal authority is a common part of VANET models[10]. Despite each country having different rules and regulations it has two main tasks – Vehicle Registration, Offence Reporting. After manufacturing of every vehicle in administrative region gets license plate issued. TTP is also part of this environment which offer services like credential management or timestamping. Service providers are also importantly considered in VANET and offers services like Location Based Services (LBS) and Digital Video Broadcasting (DVB)[7].

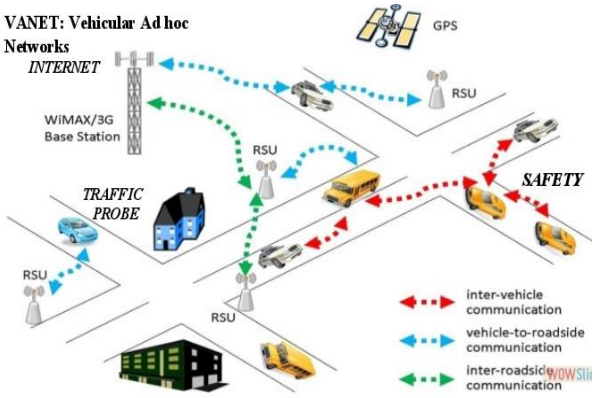

Figure 1: Architecture of VANETs[1]

b) Adhoc Environment:- In this type of network periodic communication among vehicles and RSU are established. Vehicles are normally equipped with three basic devices . Firstly, they are equipped with communication unit that is named as On Board Unit (OBU) for V2V and V2I communication. Then they have a set of sensors to judge their own status and environment[7]. Sensor information can be useful to share with other vehicle in the network to increase road safety. Finally Trusted Platform Module (TPM) are mounted on vehicles and are used for security purposes. This devices is used for reliable storage and computation and is tamper-evident information such as user credentials and pre crash information can be stored in turn[8][10].

II. DENIAL OF SERVICE (DOS) ATTACKS

In Denial of Service (DoS) attack, the attacker attacks the communication medium to create channel jam or to stop nodes from accessing the network[13]. The basic idea is to flood the network with excessive traffic and to make network and resources unavailable for legitimate nodes. This will result in devastation and overtiredness of the vehicle nodes and network resources. The network will be not able to perform accurately and will deny services to authentic nodes and will perform some other irrelevant functions[2].

DoS attacks can be performed by network insiders and outsiders and make network unavailable to authentic users by flooding control channel with high speed malicious messages. DoS attack majorly effects key resources which include bandwidth, CPU and memory, There are three ways by which attackers may achieve DoS attacks named as communication channel jamming, network overloading, packet dropping. The various levels of DoS attacks are detailed below:-

A. Basic Level: Overwhelm the Node Resources:- This is the basic level of DoS attack in which the main goal of attacker is to occupy the node resources such that the node cannot perform other necessary and important operations. The node become busy and uses all the resources to verify messages[2].

- *Case 1:- DoS attack in V2V Communication:-* In this case attacker send warning message related to accidents at some location. A node behind the attacker node is a victim node which receives this message. However, the sender keep on sending this message continuously thus to keep the victim node busy and will completely denied using network.

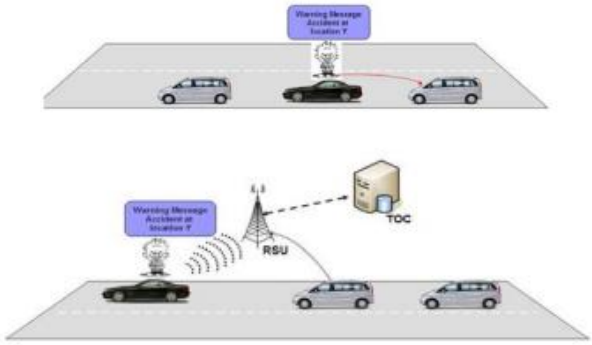

Fig 2: DoS attacks in a) V2V Communication, b) V2I Communication

- *Case 2:- DoS attack in V2I Communication:-* In this case the attacker attack RSU (Road Side Unit) as shown in figure 3. Due to attack, RSU will be busy in verifying messages and any other node who wants to communicate with RSU will not be able to do the same making RSU unavailable to the users. Hence, sending information related to critical life safety in this case is very risky[2].

B. Extended Level:- Jamming the channel:- In this attack, the attacker jams the channel and not allow the other users/to access the network nodes.

- Case 1:- In this case attacker jams the communication between any vehicles randomly by sending high frequency channel. Vehicles in this domain will not be able to send or receive messages due to this attack. They can send/receive messages once they leaves this domain of attack[2].

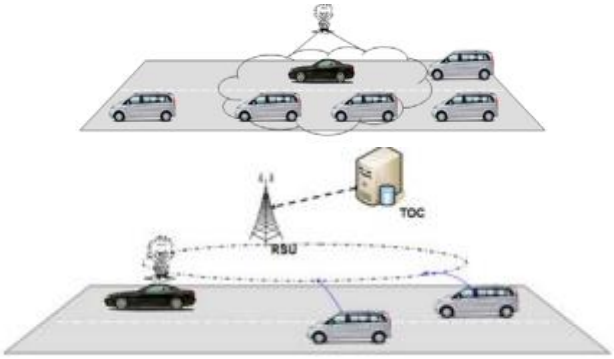

Fig 3: Jamming in a) V2V Communication b) V2I Communication

- Case 2:- In this case attacker jams the communication channel between the vehicles and the RSU or infrastructure. In this situation, attacker attack the infrastructure to jam channel because of this sending or receiving of messages to/from the nodes and the RSU is not possible due to unavailable network[2].

III. EXISTING PACKET DETECTION ALGORITHMS

A. *Attacked Packet Detection Algorithm (APDA)*
In this, each RSU is equipped with this mechanism. All vehicles can communicate with RSU through APDA mechanism. Its main work is to detect certain position of vehicles. Once the positions has been detected, it is then stored in the certain RSU. Devices like OBU and TAMPERPROOF are mounted on each vehicle and store detailed information about the vehicles like speed, position. OBU, frequency, velocity of the vehicles actually help in identifying the position of vehicles in the network. APDA algorithm is responsible to detect the packet send by vehicles and the position of the vehicles. If it is found, the packet is attacked then vehicle will be tracked else not[4].

B. *Enhanced Attacked Packet Detection Algorithm (EAPDA)*
In this model, communication takes place through RSU using control packets. RSU performed vehicle request and verification by using EAPDA algorithm. Only vehicles those are verified by RSU will be provided services and network resources and all the nodes will be rejected for using any resources of the network as are responsible for DoS attack by flooding communication channel. This will increase availability of the network resources to legitimate nodes, thereby increasing the output of network. The DoS attackers are detected during the verification phase. To be able to allot time slot to all the nodes, RSU calculate the time at which request is send and received as well as the number of vehicles who send the request. The RSU use vehicle id to trace vehicles future requests. In allotted time. RSU will analyze each node on the basis of number of packets being transferred from it. If the packet sending rate is greater than the threshold value then that node is detected as malicious node which needs to be removed from network for effective communication[3].

C. *Malicious and Irrelevant Packet Detection Algorithm (MIPDA)*
This algorithm is enhanced version of APDA. Like APDA, it detects the malicious nodes and packets on the basis of frequency, velocity, speed and road characteristics. Unlike APDA, it detects the real packets by taking into account the values of frequency and velocity. This algorithm increases the security of system, decreases the delay and overhead [5].

IV. PROPOSED ALGORITHM

This algorithm will help the networks to avid DoS attacks and if the network is attacked by the malicious nodes, then this algorithm will detect the malicious nodes and discard all the packets sent by them in the network. So, this algorithm will help m making available the network all the time for the dissemination of critical life related information.

This mechanism will help in detection of malicious nodes by detecting the irrelevant packets with the help of Road Side Units (RSU). Each node will communicate through RSU which will help the RSU to save the information of each vehicle. Then, when any node sends the harmful messages, that vehicle can be detected and checked with the help of information of its location in RSU. This algorithm can detect multiple malicious nodes and irrelevant packets sent by them in the network. This algorithm is under the category of packet detection algorithm.

A. Algorithm 1: Identification of Multiple Malicious Nodes

Input: Frequency (freq), Velocity (vel), multiple number of nodes (N), threshold value range of freq and vel (low, high)

1. **Identify** (Malicious Packets and nodes)
2. **Begin**
3. RSU will track all nodes in the network
3. **if** freq and vel both high for multiple nodes
   packet is from malicious node.
4. track that malicious vehicle.
5. drop all the packets sent from them.
6. **Else if** freq and vel both are low,
7. packet is irrelevant
8 **Else** freq and vel is between high and low
9. packets are genuine and disseminated into network.
10. **End if**
11.**End if**
12. **End**

Algorithm 1 clearly identifies the malicious nodes from the multiple nodes in the network. When the multiple nodes try to disseminate some information in the network , they always communicate through RSU. RSU will check the frequency and velocity of each node in the network and will compare that values of frequencies and velocities with the upper and lower bound of the threshold.

If the freq and vel of node is high, that is approximately double than the specified range, then that nodes are specified as malicious nodes. Those nodes can create DoS attacks, so they need to be isolated as soon as possible. These nodes are tracked by the RSU for their location and also for the messages that are disseminated by them in the network. and after their tracking, these nodes are isolated from the network and are stopped for sending any packets to the legitimate users.

If the freq and vel both are low, the packets are irrelevant and will not be forwarded in the network to the legitimate users. These packets are send by the malicious nodes for jamming the channels and can result in DoS attack an y time.

If both the freq and vel are low, then these packets are not from malicious nodes but, they have some important information related to the network node or the traffic ahead, weather conditions. So, all the packets with this configuration are forwarded as such in the network to all nodes.

So with the proposed algorithm, we can detect multiple malicious nodes and we can differentiate between the nodes who are sending the malicious and irrelevant packets and genuine packets in the network respectively.

The performance parameters used for the evaluation of this work are:-

a) Packet Loss:- It is the ratio between the packets loss and the total packets seny by any node to the destination. Its value depends upon the congestion in the netwok due to which packets fail to reach their destination successfully[12][14].

b) Lifetime of network:- Lifetime of a network is defined as time during which the vehicles of the network are able to route information successfully.If any number of nodes are out of energy or loose some fuctionality due to any reason,then the lifetime of the network ends.

c) Network Throughput:- It is defined as the percentage of data sent from the source to destination in given time. The high the throughput value,the maximum information is transmitted between source and destination.

d) Packet Delivery Ratio:- It is defined as the number of packets that are delivered to the destination in comparision to the number of packets send by the source for destination[14].

e) Number of dead and alive nodes:- It is the number of nodes which stop working are considered as dead nodes and the number of nodes which are disseminated the information in the network are under the alive nodes,

The entire simulation was done in NS-2. Since the network has to deal with multiple nodes, so the first simulation is done with only 5 nodes in the network as shown in Figure 4

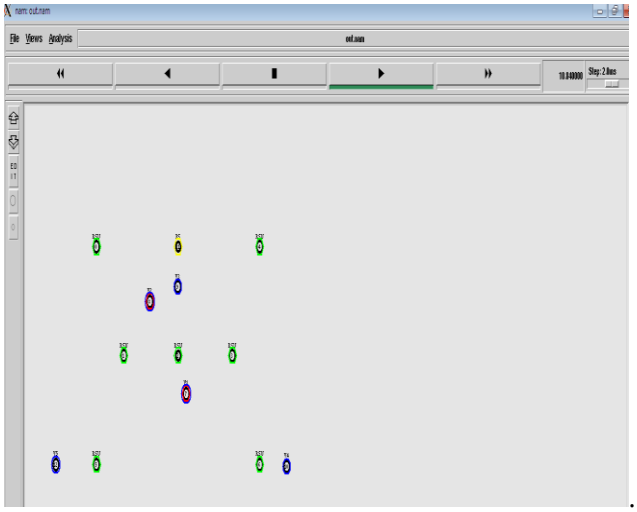

Figure 4: Multiple nodes in simulation environment

Figure 4 shows the simulation screen in NS-2 which contains number of nodes in the network. All the nodes will communicate with each other by disseminating useful information through RSU.

The network throughput is shown in Figure 5 which is measured n Gbps (Gigabits per second). and Figure 6 shows the network lifetime of the network which is increased as the multiple malicious nodes are detected well in time that is during verification time. The network lifetime of the network depends on the time when the network is fully operative.

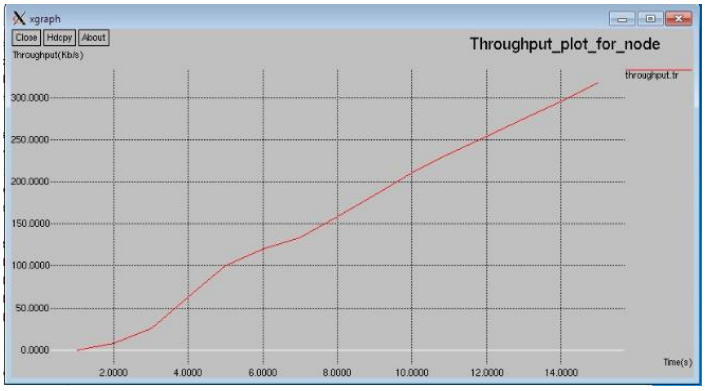

Figure 5: Network Throughput with 5 nodes in network

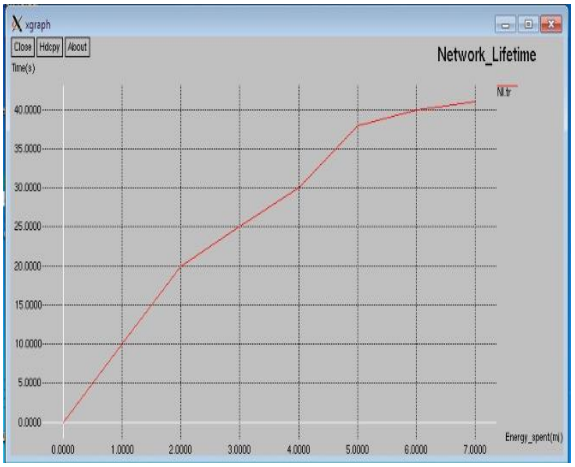

Figure 6: Network Lifetime

The packet delivery ratio is shown in Figure 7. The graph shows that the packets sent by the sender for destination does not received fully by the destination. Another parameter for the evaluation was packet loss ratio. The packet loss ratio clearly defines the number of packets which does not reach for the destination but are sent by the sender which is shown in Figure 8. Packet Delivery ratio is increased in comparison with the existing techniques that is number of packets that are delivered to the destination from the source is increased. Packet Loss Ratio is decreased as the delivery ratio is increased, the loss ratio will be decreased. That is, the number of packets that are lost during the communication process is very less and all the useful information is disseminated in the network effectively.

Figure 7: Packet Delivery Ratio

Figure 8: Packet Loss Ratio

The proposed algorithm for detection of multiple malicious nodes is simulated using different number of nodes that is taking 5, 8, 10 and 12 number of nodes. Figure 9 shows the simulation of 12 nodes with multiple RSUs.

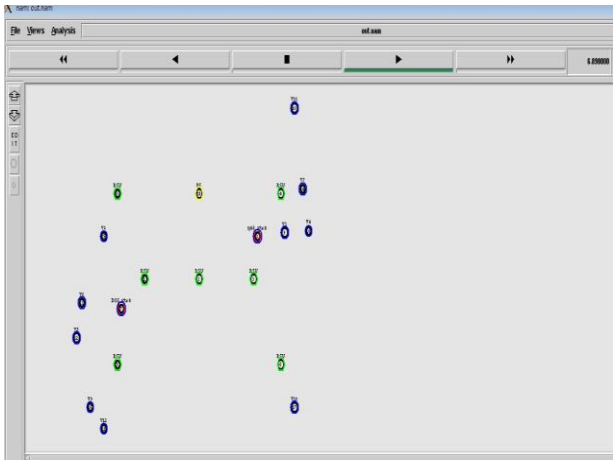

Figure 9: Simulation with 12 nodes

The values of performance parameters that are throughput of the network, packet delivery ratio, packet loss ratio and network life time is given in Table 1.

Table 1: Performance Parameters Table

Number of nodes	Throughput of network	Packet Delivery Ratio	Packet Loss Ratio	Network Life time
5	250	58	300	41
8	300	59	190	39
10	350	62	152	38
12	360	68	130	37.5

The comparison of the proposed technique is also done with the exiting technique which is shown in Table 2.

Table 2: Comparison Table

Parameters/ Attacks	Previous work with 1 node	Proposed work with 5 nodes	Proposed work with 8 nodes	Proposed work with 10 nodes	Proposed work with 12 nodes
Throughput	190	250	300	350	360
Packet Delivery Ratio	38	58	59	62	68
Network Lifetime	43	41	39	38	37.5
Packet Loss Ratio	146	300	190	152	130
Sybil and DoS Attack	DoS Attack Detection	DoS Attack Detection	DoS Attack Detection	DoS Attack Detection	Sybil & DoS Attack Detection

The existing algorithm was able to detect single malicious node at one time. Also the RSU was not able to track number of vehicles at same time. But the proposed algorithm is capable of checking multiple malicious nodes at same time and also RSU can communicate with number of nodes at the same time. The proposed technique is capable for detecting Sybil as well as DoS attacks if implementing on 12 nodes but all other techniques can only detect DoS attack.

All the calculated parameters show that the proposed algorithm is far better than the existing one. The throughput of the network is increased; packet delivery ratio is also increased. Although the network lifetime is decreased slightly but the packet loss ratio is decreased dramatically.

V. CONCLUSION

In this paper, the nodes which are responsible for attacking the network are detected on the basis of frequency and velocity. Both the irrelevant packets as well as genuine packets are detected by this algorithm. The algorithm is able to detect multiple nodes which are attacking the network rather than the single node as by the existing algorithms. By detection of attacker nodes well in time, the lifetime of the network is increased. Other performance parameters also show effective difference in their values which proves that the proposed algorithm is improved version of existing packet detection algorithms.

ACKNOWLEDGMENT

Authors are highly thankful to the RIC department of IKG Punjab Technical University, Kapurthala, Punjab, India for providing the opportunity to conduct this research work.

VI. REFERENCES

[1] R. Fotohi , Y. Ebazadeh , M. Seyyar , "A New Approach for improvement security against DoS attacks in Vehicular Adhoc Network" IJACSA, Vol 7, No.7, 2016, pp 10-16.

[2] H. Hasbullah, I. Soomro, J. Manan, " Denial of Service (DoS) attack and its possible solutions in VANET", World Academy of Science, Engg, & Tech., IJECE, Vol 4, Issue 5, 2010, DOI scholar.waset.org/1307-6872/15804.

[3] A. Singh, and P. Sharma, "A novel mechanism for detecting DOS Attack in VANET using Enhanced Attacked Packet Detection Algorithm" Proc. IEEE International Conference RACES,21-22 December, 2015, doi 10.1109/RACES.2015.7453358.

[4] S. RoselinMary , M Maheshwari ., M. Thamaraiselvan , "Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA)" Proc. IEEE, ICICES, February 2013, doi 10.1109/ICICES.2013.6508250.

[5] A. Quyoom, Ali, N. Gouttam , H Sharma ,"A Novel Mechanism of Detection of Denial of Service Attack in VANET using Malicious and Irrelevant Packet Detection Algorithm,'' Proc. IEEE in ICCCA ,pp.414-419, IEEE 2015, doi 10.1109/CCAA.2015.7148411.

[6] K.Thilak,"DoS attack in VANET Routing and possible defending solutions – a survey", Proc in Int Conf on Information Communication and Embedded Systems, IEEE, 2016 doi 10.1109/ICICES.2016.7518892.

[7] J. Fuentes, A. Tablas, A. Ribagorda,"Overview of security issues in Vehicular Adhoc Networks", Handbook of Research on Mobility and Computing, IGI Global, 2010.

[8] P. Papadimitratos, L.Buttyan,J.Hubaux,"Architecture for Secure and Private Vehicular Communcations, 7th International Conference on ITS, pp 1-6.

[9] S. Zeadally, R. Hunt, Y. Chen,A. Irwin, A. Hassan,"Vehicular Adhoc Networks (VANETs):status, results and challenges,"Springer Science and Business Media, LLC 2010, pp 217-241, doi 10.1007/s11235-010-9400-5.

[10] A. Sari, O. Onursal, M.Akkaya, "Review of the Security Issues in Vehicular Adhoc Networks (VANETs)" Int J. Communications, Network and System Sciences, 2015, Vol 8, pp 552-566, doi 10.4236/ijcns.2015.813050.

[11] A. Malla , R Sahu ., "Security Attacks with an effective solution for DoS attacks in VANETs" IJCA(0975-8887), Vol 66, No 22, March 2013, pp 45-49.

[12] B. Mokhtar, M. Azab, "Survey on Securiy Issues in Vehicular Adhoc Networks" Alexandria Engineering Journal, Science Direct, Vol. 54, Issue 4, December 2015, pp 1115-1126.

[13] V. La, A. Cavalli,"Security attacks and solutions in Vehicular Adhoc Networks – A Survey" Int Journal of Adhoc Networking System, Vol. 4, No. 2, April 2014, doi 10.5121/ijans.2014.4201.

[14] J. Nethravathy, G. Maragatham,"Identifying Malicious Nodes and Performance Analysis in VANET" Int Journal of Applied Engineering Research, Vol. 11, No. 9 (2016), pp 6716-6719.