Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.8, No.6, 2018

An Innovative Technique to Avoid Traffic Jamming for VANET Using NS-2

Pooja Kourav*
PG Scholar, CSE, VITS, Bhopal, India

Prof. Sumit Sharma
HOD CSE, VITS, Bhopal, India

Abstract

A range of efficient control of vehicles has grown together with information and communication tools In scrupulous, with the appliance of wireless network for real world information offering, it has been feasible to create Vehicular Ad-hoc Network (VANET), an intellectual vehicle service for ease and protection, which does feasible crash accident detection and prevention, caution of hazardous aspects on road, traffic information offering, and other types of service offering. Nevertheless, the VANET service situation has physical and technical vulnerabilities sourced by the vehicular inside/outside communication based on wireless network. Thus, Vehicular protection has become known as a crucial aspect to avert malevolent threats and confidentiality defiance from vehicles, drivers, and traffic network. In this paper we proposed a scheme for discovering the routing mischief of an attacker aligned with traffic jamming. Now if the congestions take place in a particular section then in that case all vehicular nodes would produce the traffic jam indications known as Jamming declaration indications to their fellow vehicles and through that the vehicular node would modify their direction. Performances of outcomes are calculated on the basis of parameters: Packet Delivery Ratio, Routing Load and Throughput using Network Simulator (NS-2).

Keywords: VANET (Vehicular Ad-hoc Network), Vehicle security, traffic jamming, Road Side Unit

I. INTRODUCTION

Vehicular Adhoc networks (VANETs) are a subgroup of Mobile Adhoc Networks (MANETs) with the distinctive property that the nodes of network are vehicles like cars, trucks, buses and motorcycles. This means that node movement is restricted by factors like a road course, encompassing traffic and traffic laws. Attributable to the restricted node movement it's a possible assumption that the VANET are going to be supported by any fixed infrastructure that facilitates with some services and might offer access to stationary networks. The fixed infrastructures are planning to be deployed at important locations like service stations, dangerous intersections or places well-known for venturesome atmospheric condition.

VANET is abbreviation for Vehicular Ad hoc Network [1]. Vehicular Ad-Hoc Networks (VANETs) are a subclass of Mobile Adhoc Networks (MANETs) where movable nodes are self organized and self managed in a scattered manner. They accommodate vehicles units and/or roadside units that facilitate inside the network plays a very significant role for the Security of system with the occurrence of VANETs. Caused by the untrustworthy communications in VANETs, defense protocols would similar to a lot of anxieties, similar to confidentiality, validation, and reliability of messages. Nevertheless, the effectiveness was unobserved earlier than as a result of prior techniques acquire significant communication upward. A number of Intrusion Detection methods for VANETs are estimated. Nevertheless, not affecting imagines vehicles and vehicles with a believable eminence model aren't attention concerning in different approaches. Fig. 1 represents the VANETs.

Vehicular Ad-hoc Network (VANET) can be envisaged as the network of moving vehicles act in asynchronous and autonomous fashion. Economical and scalable data disseminated may be a major challenge because of the movement of vehicles that causes unpredictable changes in topology. For people living in developing countries the sheer volume of road traffic is also a daily nuisance. The road traffic conditions have an effect on the protection of the population since one point two million people worldwide are calculable to be killed once a year on the roads. For this reason, these days the motorcar motive business and governments invest several resources to extend road safety and traffic potency, in addition on cut back the impact of transportation on the setting. The appliance of communications and knowledge technologies for this purpose has opened a replacement variety of possibilities. One amongst the foremost promising areas of analysis is that the study of the communications among vehicles and roadside units, or additional specifically the transport Adhoc Networks (VANET) this sort of networks are self-configuring networks composed of a group of vehicles associated components of roadside infrastructure connected with one another while not requiring an underlying infrastructure, causing and receiving info and warnings concerning the present traffic situation.

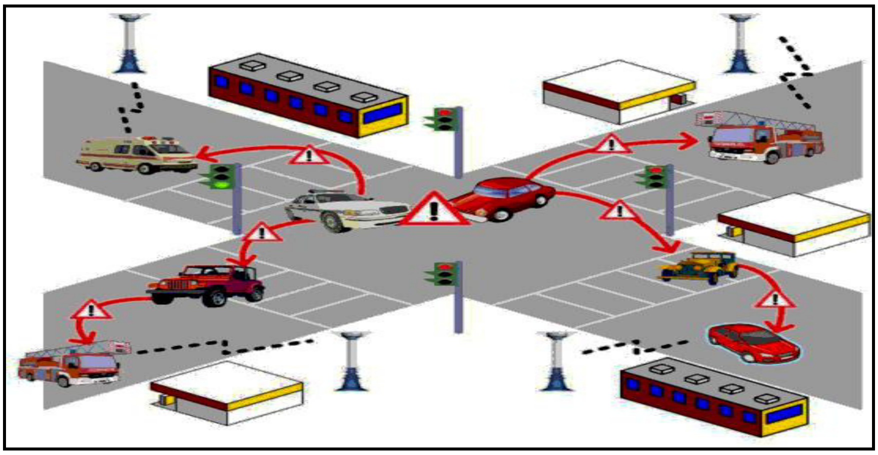

Figure 1: Vehicular Ad-hoc networks

Nodes are expected to speak by suggesting that of North Yankee DSRC normal that employs the IEEE 802.11p normal for wireless communication. To permit communication with participants out of radio vary, messages have to be compelled to be forwarded by alternative nodes (multi-hop communication). Vehicles aren't subject to the strict energy, house and computing capability restrictions usually adopted for MANETs. Tougher is that the doubtless terribly high speed of the nodes (up to 250 km/h) and also the massive dimensions of the VANET.

The primary VANET's goal is to extend road safety [2]. To attain this, the vehicles act as sensors and exchange warnings or a lot of typically "telematics" info (like current speed, location or second sight activity) that permits the drivers to react early to abnormal and doubtless dangerous things like accidents, traffic jams or glaze. The data provided by alternative vehicles and stationary infrastructure may also be used for driver facilitate systems like adaptations controller (ACC) or breaking facilitates. Additionally, approved entities like police or firefighters ought to be ready to send alarm signals and directions e.g. to clear their method or stop alternative road users. Besides that, the VANET ought to increase comfort by suggesting that of added services like location primarily based services or net on the road.

The life-or-death risk may be the most special feature of VANETs. In the traditional networks or other emerging mobile networks, security and privacy failures usually bring only financial losses. However, both security and privacy failures in VANETs could be much more serious. For instance, the failure to notice a tampered transport message in time could cause serious traffic accidents, with loss of lives. In case of privacy not closer, a driver (e.g. A widely known rich person or picture star) could become the victim of kidnappers for ransom if organized criminals extract his/her driving routine by aggregation and analyzing conveyance communications. This implies that every effort must be devoted to security and privacy concerns as a precondition for wide adoption of VANETs. To achieve security, mechanisms area unit needed to ensure authentication, integrity and non-repudiation of conveyance messages [2]. At now, one realizes that determination the inherent conflict between authentication and privacy poses a big challenge.

We found that network availability has been directly affected in the case of DOS attacks, where the attack has led to most severe impact by causing the network to break down. This type of attack is the major reason of traffic jamming in a particular route. The attacker continuously forwarded the positive message to vehicles by that they follow the congested route.

VANET is vulnerable to several attacks. Attackers, by using these vulnerabilities, can reduce the performance of the network and cause serious problems for legitimate users to use VANET based service. The goal of the attacker is to overwhelm the node resources such that the nodes cannot perform other important and necessary tasks. The node becomes continuously busy and utilizes all the resources to verify the messages. DDOS attacker jams the channel for transferring false information packets in VANET, thus not allowing other users to access the network. During this paper we work on security problems jointly on the foremost necessary issues in the transport unplanned network.

Rest of the paper is organized as following: in section II we explained Security need of VANET, in section III research conducted by different researchers on security issues on VANET had been summarized, The proposed method and its algorithm is given in section IV, in section V Results of proposed method is demonstrated and compared, lastly in section VI we concluded our work.

II. SECURITY CHALLENGES IN VANET

VANET poses a number of the foremost difficult issues in wireless ad hoc and detector network analysis. additionally, the problems on VANET security become more challenging [2] due to the distinctive options of the network, like high-speed quality of network entity or vehicle, and extremely great amount of network entities specifically, it's essential to create sure that “life-critical safety” data can't be inserted or changed by an attacker; likewise, the system ought to be ready to help establishing the liability of drivers; however at a similar time, it ought to protect as way as possible the privacy of the drivers and passengers. It is obvious that any malicious behavior of users, like a modification and replay attack with regard to the disseminated messages, might be fatal to alternative users [3]. Within the past few years, considerable effort has been spent in analysis on VANET networking protocols and applications. However, analysis on security threats and solutions and reliability of VANET solely started recently, e.g. [4]. Summarizing from the recent researches on top of, VANET security ought to satisfy the following needs.

Message Authentication and Integrity: Message should be protected against any alteration and therefore the receiver of a message should corroborate the sender of the message. However integrity doesn't essentially imply identification of the sender of the message.

Message Non-Repudiation: The sender cannot deny of sent an information message.

Entity Authentication: The receiver isn't solely ensured that the sender generated a message, however additionally has evidence of the aliveness of the sender.

Access Control: Access to specific services provided by the infrastructure nodes, or different nodes, is decided locally by police. As a part of access management, authorization establishes what every node is allowed to try and do in VANET.

Message Confidentiality: The information of a message is kept secret from unauthorized to access it.

Availability: The network and applications ought to stay operational even within the presence of faults or malicious conditions. This means not solely secure however additionally fault-tolerant styles, resilience to resource depletion attacks, further as survivable protocols that resume their traditional operations when the removal of the faulty participants.

Privacy and Anonymity: Conditional privacy should be achieved within the sense that the user connected info, as well as the driver’s name, the license plate, speed, position, and traveling routes at the side of their relationships, has got to be protected; whereas the authorities ought to be ready to reveal the identities of message senders within the case of a dispute like a crime/car accident scene investigation, which may be accustomed hunt for witnesses.

Liability Identification: Users of vehicles are liable for their deliberate or accidental actions that disrupt the operation of other nodes, or the transportation system. Several attacks are known which will be classified depending on the layer the attacker uses. At the physical layer and link layers the attacker will disturb the system either by jamming or overloading the channel with messages. Flooding false messages or rebroadcasting a recent message is also an attainable attack. The attacker may steal or tamper with an automobile system OBU or destroy a roadside unit. At the network layer the attacker can flood false routing messages or overload the system with routing messages. The attacker may also compromise the privacy of drivers by revealing and tracking their positions. The same attacks can also be achieved using the application layer. In the following, we summarize the major vulnerabilities and security threats of VANET.

Jamming: The jammer deliberately generates interfering transmissions that prevent communication within their reception range. In the VANET Situation, an attacker can relatively easily partition the network, without compromising cryptographic mechanisms and with limited transmission power.

Impersonation: An attacker can masquerade as an emergency vehicle to mislead other vehicles to slow down and yield. An adversary can also impersonate Road Side Units, spoofing service advertisements or safety messages. So an impersonator can be a threat. Message fabrication, alteration, and replay can all be used towards impersonation.

Privacy Violation: The collection of vehicle-specific information from overheard vehicular communications will be very easy with VANET deployed. Then inferences on the personal data of drivers could be made, thus violate the privacy of drivers.

Forgery: An attacker can forge and transmit false hazard warning information or other messages, and it can rapidly contaminate the large portions of the VANET coverage area. The correctness and timely receipt of application data is a major vulnerability.

In-transit Traffic Tampering: A node acting as a relay can disrupt communications of another node. It can drop or meaningfully modify messages. Attackers can also answer messages, e.g., to illegitimately obtain services like traversing a toll check purpose. Tampering with in-transit messages could also be easier and a lot of powerful than forgery attacks.

On-board Tampering: The attacker might choose to tinker with data, e.g., velocity, location, standing of vehicle components at their source, tampering with the OBU sensing and different hardware. In fact, it may be less complicated to exchange or by-pass the real-time clock or the wiring of a sensor, instead of modifying the code implementation of the data collection and communication protocols.

III. LITERATURE SURVEY

Researchers are continuously working on Security in VANET communication, finding ways out of this very critical problem and a number of techniques are proposed by the research community. Very few of them are described here:

Feng Zhang et.al [5] presents a traffic information aggregation and propagation scheme, which is suitable for the urban environment and based on Vehicle Ad hoc Network (VANET) to improve the traffic condition. Roadside units (RSUs) can collect, generate and distribute traffic messages, using v2v communication and vehicles mutual collaborate. The traffic information can help drivers to choose a better route and prepare against the traffic events. It's advantageous to avoid traffic jam and reduce the occurrence of traffic accidents. But in this paper author not show the effect of attack by that the jamming is occur because to identify attacker is a difficult issue that one is the main cause of jamming.

Zeadally. S. et.al. [3] Vehicular ad hoc networks (VANETs) have attracted a lot of attention over the last few years. They have become a fundamental component of many intelligent transportation systems and VANETs are being used to improve road safety and enable a wide variety of value-added services. Many forms of attacks against VANETs have emerged recently that attempt to compromise the security of such networks. The authors discuss some of the main security threats and attacks that can be exploited in VANETs and present the corresponding security solutions that can be implemented to thwart those attacks..

Irshad Ahemed Sumra et.al [6] proposes five different classes of attacks and every class is expected to provide better perspective for the VANET security. The main role of this paper is the proposed solution for classification and identification of different attacks in VANET.

Farjad Sabahi et.al [7] integrates mobile connectivity protocols to prompt data transfer between vehicles as well as between roadside unit and existing traffic in the network. In VANET, Wireless node with devices sends information to neighbor vehicles, and messages can be transmit from one vehicle to other vehicle. Therefore, using VANET can augmentation safety and traffic optimization. Just the same other technology, in VANET there are some important and noteworthy issues. In this paper, try to discuss security issues as one of the most important problems in Vehicular Ad hoc network.

C.-L. Huanget,al [8] design a cross layer control system where the objective is to not improve the efficiency of the MAC but to improve the vehicle tracking accuracy. The authors consider a lossy shared channel where increased message frequency can increase the channel jamming and effectively cause a loss in accuracy of other vehicles' positions. The proposed algorithm is a method to adapt the periodicity of transmission to attain the optimal accuracy.

J. B. Kenney [9] proposed a jamming control mechanism where the packet injection rate is controlled to attain a given target channel load. However, the issues of discovery performance as well as the choice of the optimal channel load are not explicitly considered.

S.Sharma, M.AL-Shurman et.al.[10][11] said The black hole attack is one of the security attacks that occur in MANETs which can occur in VANETs as well. A black hole is formed when nodes refuse to participate in the network or when an established node drops out. In this type of attacks, all network traffics are redirected to a conspicuous node, which does not exist at all that reason those data to be lost [19]. There are two proposed possible solutions for this problem in MANETs. The protocol finds more than one route to the destination. It is clear that this solution may impose overload to network. In addition, this solution may be useful in MANETs but for VANETs which has several mobile nodes, finding spare node increases unwanted parameters such as cost of service. The second solution is to exploit the packet sequence number included in any packet header [20].

Ilias Leontiadis,Cecilia Mascolo et.al. [12][13][14] have been proposed some approaches which are using publish/subscribe paradigm for information dissemination in VANET like settings. These approaches have contributed significantly towards understanding the applicability of publish/subscribe over VANET. In these approaches, a hybrid setup is assumed where there are stationary info-stations and moving vehicles communicating in cooperative manner. The main goal is to design a P/S middleware for vehicular networks that considers location and time in its design objectives. This middleware enables the application developers to easily publish notification in specific location by treating location as context. It takes advantage of the information that can be extracted from the vehicle's navigation systems (location, map, destination of the driver etc.) to generate subscriptions. Navigation system decides if a vehicle is interested on receiving a specific notification or not. Proposed system is an opportunistic Publish/Subscribe system.

IV. PROPOSED METHOD

In this Paper we proposed "An Innovative Technique to Avoid Traffic Jamming for VANET Using Ns-2". The vehicles are travelling in a single pathway to providing the data/message regarding the traffic to all vehicles and the source of every vehicle is same visibly revealed in Fig. 2. In ordinary situation every vehicle pursues the regulations and transmitting accurate data/message in communications regarding the traffic but a hacker throws multiple forged requests to a number of victim's vehicles in network, grueling all of the victim's vehicles resources and avoiding the usages via authentic vehicles.

In this paper we proposed a scheme for discovering the routing mischief of an attacker aligned with traffic jamming. Now if the congestions take place in a particular section then in that case all vehicular nodes would produce the traffic jam indications known as Jamming declaration indications to their fellow vehicles and through that the vehicular node would modify their direction.

However, the attacker node would constantly transmit the precise message regarding the traffic by that jam will take place. The proposed technique offers the resolution to theses attacks, in which the objective is to make sure that the network accessibility for protected communication among all the nodes is available. We discover that network accessibility has been directly influenced in the case of DDOS attack, where the assaults have led to most harsh influence by causing the network to collapse. We characterize the proposed process done by Road Side Unit (RSU) to defend traffic from jamming. Through above process we might identify attacker vehicle and pertaining prevention of these molests in the network.

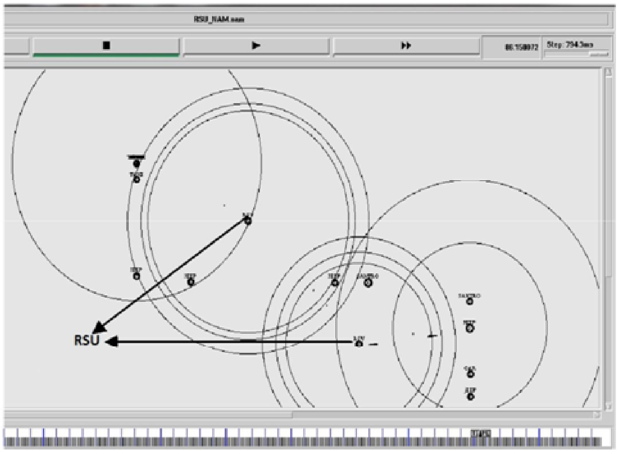

Figure 2: Situation without Traffic Jamming

Now two different circumstances illustrates the data/message regarding the traffic at the occurrence of traffic jamming and the subsequently circumstances is explained the data/message regarding the traffic clearance via stop the reason of the attacker. The particular circumstances are having the seven fields that demonstrate the data/message regarding the attacker forged packet information and the succeeding is a case of attacker identification and removal.

Road-Side Unites (RSUs) is obligatory modules in VANET. The rationales of the RSUs are to

a) Circulate the information to nearer vehicles
b) Accumulate information to the core offices
c) To supply Internet link and pursuit to the travelers.

These RSUs are wireless Base Stations, Wireless Access Point (WAP) or AP for short. They are utilized to transmit and obtain information from the integrated VANET controller in all vehicles. Therefore, the usual inquiry is: why not we utilize these RSUs to supply secretive, economical, and perfect positioning structure for the vehicles.

4.1 Proposed Algorithm

Below we explain propose security algorithm.

- **STEP 1:** set verbose ON
- **STEP 2:** set an_id [expr $val(nn) - 1]
- **STEP 3:** set total_host 200000
- **STEP 4:** set probing_port [Application/Worm set ScanPort]
- **STEP 5:** probing packet size
- **STEP 6:** slammer worm UDP packets of 404 Bytes
- **STEP 7:** set p_size 404
- **STEP 8:** Application/Worm set ScanPacketSize $p_size
- **STEP 9:** Agent/MessagePassing set packetSize_ $p_size

#set verbose ON
set an_id [expr $val(nn) - 1]

"The significance of this remarked syntax to set off the forged activities of the malevolent vehicle to spread the virus in the network and the "an" symbolizes the "abstract network" it signifies that network influenced from virus apart from the attacker."

set total_host 20000

"The significance of this statement is to the attacker visualize, that the number of movable nodes in nodes or hosts in network are 20000."

set probing_port [Application/Worm set ScanPort]

"Any host in network are identifies the receiver node on the basis of port number, this is the number of category of protocol. So here as well the attacker having a port number through that the other hosts are agrees to the information generated by attacker at application layer".

# probing packet size

# slammer worm UDP packets of 404 Bytes

set p_size 404

Here the 404 signifies the dimension of packets and the category of packet is a UDP because of attacker nothing desire to respond from any node in the network.

Application/Worm set ScanPacketSize $p_size

"The scan rate of packets are stated on the basis of number of packets are sent in network per second for application protocol."

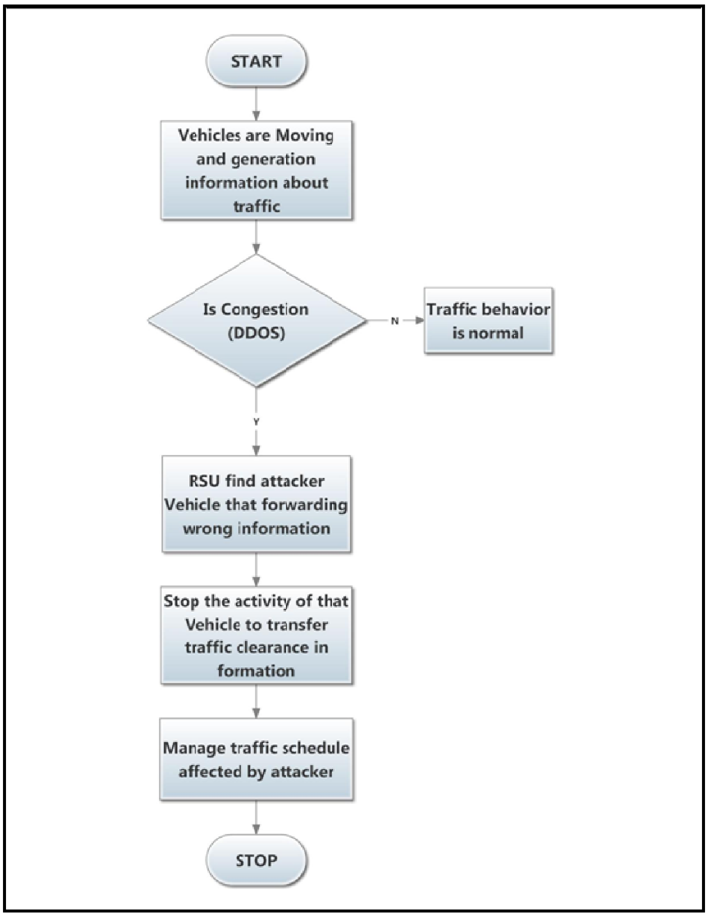
START
Vehicles are Moving and generation information about traffic
Is Congestion (DDOS)
N
Traffic behavior is normal
Y
RSU find attacker Vehicle that forwarding wrong information
Stop the activity of that Vehicle to transfer traffic clearance in formation
Manage traffic schedule affected by attacker
STOP

Figure 3: Flow Graph of Proposed Method

Agent/MessagePassing set packetSize_ $p_size

"Here the denotation of agent to preserve the connection among the number of nodes in the network and how much amount of information in the packets are carried in network."

4.2 Flow Graph of Proposed Method

The Flow Graph shown in Fig 3, it gives step by step procedure for Attack detection and prevention.

V. RESULT ANALYSIS

On the basis of simulation parameters given in Table I simulation has been done in ns-2 simulator (version ns - 2.31).

Table I Simulation Parameters

Number of nodes	100
Dimension of simulated area	800×800
Routing Protocol	AODV
Attacker Node	1
RSU unit	2
Simulation time (seconds)	100
Transmission Range	250m
Information Packet size (bytes)	512
Maximum Speed (m/s)	30
Nodes Mobility	Random way point

5.1 Performance Metrics

The following illustrates metrics are utilizing for difference to analysis performance:

1. ***Packet Delivery Ratio (PDR):*** The relationship of the packet sent to the destination node to the data transmits via the sender node. The PDR signify mode of victorious a protocol illustrate forwarding data from source to destination node.
2. ***Routing Load (RL):*** The number of normalized data delivered per data packet forward to the destination node. The routing load reduced is representing best result**.**
3. ***Throughput:*** Throughput is the medium speed of wealthy data forward over a communication link. A high average packet delivery network is sensible.

5.2 Performance Analysis

In this section the performance of outcomes are calculates on above mentioned parameters

a). Packet Delivery Ratio

The packets successful delivered is refining the explanations of network apart from that the data dropping is minimum the performance of network. The routing misbehavior pass by DDoS attack is decrease the 97.7% of data recognizing having number of nodes 10, 20, 30, 40 & 50 as represent in Table II. The assailant is downs whole data packets that are not delivered to destination node following approve Route Reply. The 98.7% of data successfully delivered in case of normal, attack & proposed module is shows in figure 4. The attacker has drop the greatest amount of the data packets by that the dispel performance of multipath routing is reduced.

Table II: Comparison of Packet Delivery Ration

No. of Nodes	**Percentage of Packet delivery**		
	Normal	**Attack**	**Proposed**
10	84.62	55.47	98.26
20	82.75	43.19	98.01
30	80.83	41.58	97.74
40	79.49	39.41	97.48
50	79.27	35.48	97.35

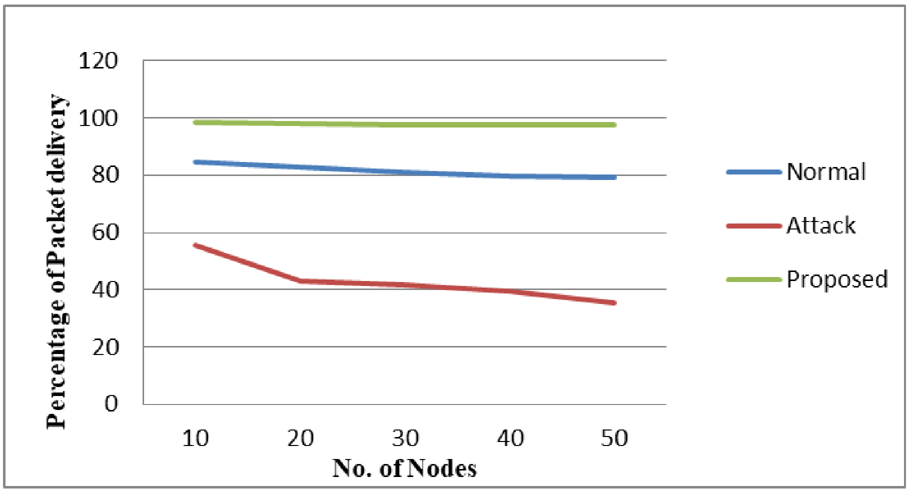

Figure 4: Analysis of Packet Delivery Ratio

b). Routing Load

The routing overhead is specify by the number of routing packets are forward in network. The routing packets are drowning in network to improvement relationship in between source and target passes by intermediate nodes. The nodes are create critical topology by that the connect growth is the testing difficulty in VANET. Table III shows the routing overload in case of Normal, Attack, & Proposed module and observe that the performance of Proposed algorithm is get better the in presence of attack environment having number of nodes 10, 20, 30, 40 and 50 nodes scenario as shown in fig 5.

Table III: Comparison of Routing Load

No. of Nodes	No. of Packets		
	Normal	Attack	Proposed
10	65	305	34
20	83	372	67
30	108	427	83
40	276	685	148
50	348	875	242

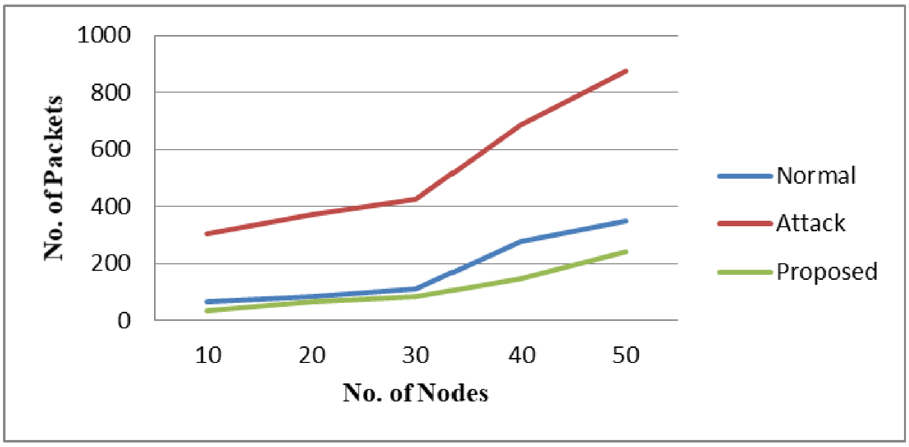

Figure.5: Analysis of Routing Load

c). Throughput

The data gathering in VANET is not unit on any management. The data delivery in this type of network is not safe. In Table IV we demonstrate the throughput analysis in case of Normal, Attack, & Proposed module. The data per unit of time in case of attacker is nearly small in network but in case of proposed safety algorithm the throughput is greater as compare to attacker having number of nodes 10, 20, 30, 40 and 50 nodes circumstances as shown in fig 6.

Table IV: Comparison of Throughput

No. of Nodes	No. of Packets		
	Normal	Attack	Proposed
10	2578	240	3872
20	1864	204	2840
30	1486	182	2743
40	1423	150	2678
50	1378	104	2536

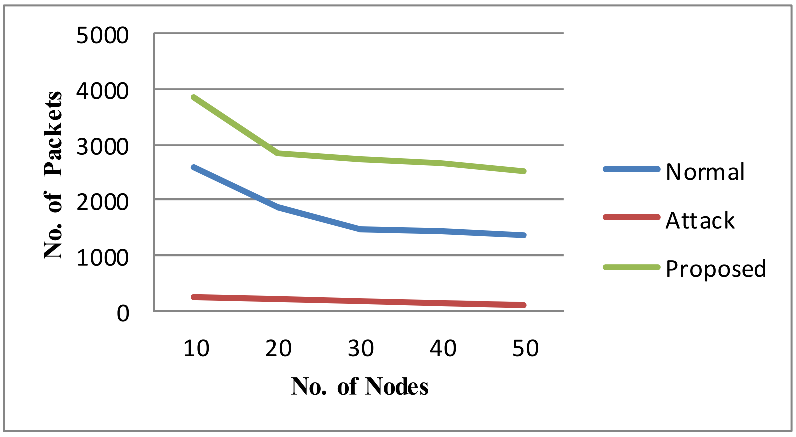

Figure 6: Analysis of Throughput

VI. CONCLUSION

From a security point of view, VANET face a number of challenges. Due to communication in wireless medium has no observable boundaries and is significantly less reliable. Wireless attacks may come from anywhere and from all directions the key objective of proposed method is offering security and console for travelers helping drivers on the roads by predicting destructive messages. Every vehicle in the presence of RSU would be a node in the Adhoc network and could accept & send further messages via wireless network. Jamming is the notice of the occurrence attacker of Road signal sections and in position of traffic sight would furnish the driver important tool to choose the greatest path along the method occurrences or awful traffic regions. The nodes in the network do not have any knowledge about attacker behavior to re-recognize them as a secure node when nodes communicating with each other for gaining traffic information. This mechanism allows maximum privacy and provides immutable identities. Now in future we also proposed location based or geographic routing. The geographic routing purposes it is usually sufficient for a node or vehicle to recognize its individual location, the location of its direct neighbors and the location of the receiving node acquired through the location service.

REFERENCES

[1.] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin and Aamir Hassan “Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges”, Springer science+Business Media, pp-217-214, Dec 2010

[2.] Stampoulis, Antonios and Zheng chai”A Survey of Security Vehiculer network” project DOI= http://zoo. cs. yale. edu/~ ams257/projects/wireless-survey. pdf (accessed: Nov 28, 2011) (2007)

[3.] Zeadally, S. , Camara, J.S. “ Security Attack and Solutions for vehicular adhoc network”, The Institute of Engineering and Technology(IET), pp.894-903,Volume 4, Issue 7,April 2010

[4.] Tim Leinmuller, Elmar Schoch, and Christian Maihofer, “Security Requirements and Solution Concepts in Vehicular Ad Hoc Networks”, Proceedings of Forth Annual Conference on Wireless on Demand Network Systems and Services Oberguyrgl, pp.84-91, 2007

[5.] Feng Zhang, Jianjun Hao and Shan Le “Traffic information aggregation and propagation scheme for vanet in city environment” 3rd IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT), pp.619-623,26-28 Oct 2010

[6.] Irshad Ahmed Sumra, Iftikhar Ahmad, Halabi Hasbullah, Jamalul-lail bin Ab Manan, “Classes of Attacks in VANET, WASET issue”,Electronic Communication & Photonic Conference (SIECPS), PP.1-5, 2011.

[7.] Farzad Sabahi “The Security of Vehicular Adhoc Networks”, Third International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN), pp-338-342, 26-28-July2011.

[8.] C.-L. Huang, Y. Fallah, R. Sengupta, and H. Krishnan.” Intervehicle transmission rate control for cooperative active safety system”. IEEE Trans. On Intelligent Transportation Systems, PP.645 –658, Sep. 2011.

[9.] J. B. Kenney, G. Bansal, and C. E. Rohrs “LIMERIC a linear message rate control algorithm for vehicular DSRC systems”, In Proceedings of the Eighth ACM international workshop on Vehicular inter-networking (VANET), pages 21–30,Sep 2011.

[10.] S. Sharma and D. R. Gupta, “Simulation Study Of Black hole Attack in the Mobile Ad hoc Networks”,Journal of Engineering Science (JEST),PP.243-250,Vol.4 no.-2,2009.

[11.] M. Al-Shurman, Seong-Moo Yoo and Seungjin Park., “Black hole attack in mobile Ad Hoc networks”, presented at the ACM Southeast Regional Conference'2004.

[12.] Ilias Leontiadis,“Publish/Subscribe Notification Middleware for Vehicular networks”, in Proceedings of the 4th on Middleware doctoral symposium, California, Article no.-12, November 2007.

[13.] Ilias Leontiadis, Cecilia Mascolo “Opportunistic Spatio-Temporal Dissemination System for Vehicular Networks”, In Proceedings of the First International Workshop on Mobile Opportunistic Networking (ACM/SIGMOBILE MobiOpp 2007), pp.39-46, USA, June 2007.

[14.] Ilias Leontiadis, Cecilia Mascolo. “GeOpps: Opportunistic Geographical Routing for Vehicular Networks”, In Proceedings of the IEEE Workshop on Autonomic and Opportunistic Communications (Colocated with WOWMOM07), Pp1– 6, Helsinki, Finland June 2007.