Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 3, June 2021:342- 362

Research Article

Approach of Malicious Nodes and Environmental in Vehicular Ad-Hoc Networks

GarimaSaini[1], Dr.Javalkar Dinesh Kumar[2]

Abstract

Vehicular Adhoc Network (VANET), a 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. The security of the nodes can be increased, if the network availability is increased. The characteristics of VANETs, such as high mobility, network partitioning, intermittent connectivity and obstacles in city environments, make routing a challenging task. Due to these characteristics of VANETs, the performance of a routing protocol is degraded. The position-based routing is considered to be the most significant approach in VANETs.

The availability of the network is decreased, if there is Denial of Service Attacks (DoS) in the network.. This technology establishes connection among cars about 100 to 300 meters of each other and, thus, generates a wide-ranging network. In the current scenario, remarkable growth in the vehicles' quantity deployed with computational tools and wireless devices has contributed in the evolution of new application strategies that were impossible in the past. in this paper , DoS affects network performance greatly with regard to throughput and other metrics. threshold- based technique is devised for eradicating adversaries from the vehicular network. The proposed algorithm was NS2 simulator for applying the new approach and outcomes are compared in terms of routing overhead, throughput and packetloss. It is analyzed that in terms of every parameter new approach works more effciently in contrast to the approaches presented in the past.

Keywords – *VANETs; DoSattacks; Packet detection; malicious nodes; irrelevant data*

[1]Research Scholar,LingayasVidhyapeeth,Faridabad, Haryana, India.
[2]Assistant Professor of Computer Science,LingayasVidyapeeth,Faridabad, Haryana, India
Received Accepted

Introduction

A Vehicular Adhoc Network (VANET) is remarkable achievement towards road safety with various state-of-artsafety applications. A VANET is self organized network which enable Vehicle-

to-Vehicle and Vehicle-to-Infrastructure communication for the exchange safety messages. This network probably will play a major role for enabling comfortable traffic system on roads and will also help in avoiding unnatural traffic mishaps. The short range radios are being installed in all the communicated nodes. The transmission range between the vehicle nodes is very short that is less than 300mThilak (2016) . Road Side Units(RSU) are installed randomly depending on the categorization of the network in that specific area. The authorities and vehicle nodes can communicate through RSU.

The automobile industry is growing day by day. Vehicular ad-hoc network (VANET) is a part of ITS which provides security, traffic efficiency and ease to the user. Vehicular network is a subclass of mobile ad-hoc network (MANET) in which vehicle acts as a mobile node in the network (Arya and Tripathi2013). Vehicles can communicate and transfer messages with other vehicles as well as roadside units using the VANET. In VANET multiple vehicles are connected in ad-hoc fashion for exchanging the useful information. VANET is the main part of Intelligence transportation system (ITS). It uses the WAVE (wireless access for the vehicular environment) technology based on the IEEE 802.11p standard (Ltifi et al. 2015). Two main parts of the vehicular network are Smart vehicles installed with the onboard unit (OBU) and roadside units. Mainly two types of communication possible in VANET first is communication between vehicle to vehicle (V2V) and second is communication between vehicle and roadside infrastructure (V2I). In VANET vehicles has a limited range for the transmission of messages, so it uses multi-hop communication to transfer the messages using different routing algorithms. In multi-hop data transfer one has to rely on other nodes also. So security and routing are the two major issues in the vehicular ad-hoc network. Every-one needs to secure the vehicular network from the insider and outsider attackers. Our proposed model detects the rouge nodes inside the network with the use of lightweight trust based algorithm. Selection of the observer node minimizes the load on all the nodes. Proposed work detects the faulty nodes with less overhead and complexity. Var-ious other proposed pre-existing models provide security with lots of complexity and overheads (Yao et al. 2017). To minimize the overhead we use the entity-centric trust-based model with the selection of the observer node. Various abbreviations used in this article are defined in Table 1.

Table 1. Abbreviation used

Abbreviation	**Full name**

VANET	Vehicular ad-hoc network
BH	Black hole
NS	Network simulator
DOS	Denial of service
AODV	Ad-hoc on-demand distance vector
PDF	Packet delivery fraction
ITS	Intelligence transportation system
DSR	Dynamic source routing
RSU	Road side unit
NRL	Normalized routing load
DSDV	Destination sequenced distance vector

Various authors (Kerrache et al. 2016a, b; Khan et al. 2015; Li and Song 2016; Ltifi et al. 2015) use the trust-based solutions to find the trustable and rouge node in the network. As trust based algorithms require fewer calculations and can per-form better if the attacker is from inside the network. In trust-based model authors mainly use the concept of direct trust, recommendation trust and historical trust (Kerrache et al. 2016a, b) as well. The other alternative security mechanism that used most widely is cryptography based model to secure the communication network. Cryptography based solution provides security from internal and outsider intruder. These types of solutions increase the complexity of the model in terms of calculation overhead. Some authors use cryptography-based solutions (Kumar and Maheshwari2014; Lim and Manivannan2016; Pooja et al. 2014) to ensure the security of the vehicular network. As we know cryptography-based solutions require more cal-culations to implement the algorithm so it creates some delay in the transfer of messages due to large calculations. But it covers all types of attacks in the vehicular network. Some authors (Khan et al. 2017; Kumar and Chilamkurti2014; Mokdad et al. 2015; Sedjelmaci et al. 2014; Tyagi and Dembla2016; Zaidi et al. 2016) proposed intrusion detection and prevention schemes to detect the faulty or attacker node present in the vehicular network.

VANET will be responsible for improved traffic safety and driver assistanceMallaet al. (2013). 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 etcZeadallyet al. (2010).The data which is received from the nodes is forwarded toother nodes after checking its reliability. The reliability ischecked by the devices acting as communicators. These needs tobe checked as the data or messages which are received are notuseful for all the nodes. The decisions

related to usefulness ofthe received data need to be made by the communicatordevicesZeadallyet al. (2010).

High mobility, dynamic mobility, regular disconnection, restricted bandwidth, attenuations, limited transmitting capacity, energy storage, and computing are just a few of the VANET characteristics that set them apart.

In the VANET model, various types of entities are involved. Vehicle nodes are the most important of the different organizations included since they perform the most basic and important roles of communication. They are capable of communicating in a variety of situations. However, in order to understand how VANET works, all of the various entities and how they communicate with one another must be thoroughly discussed and studied.

Malicious Nodes

Vehicular ad-hoc network (VANET) is the application of traditional mobile ad hoc network (MANET) in traffic road. As a new type of multi-hop wireless communication network, VANET has become a research hotspot in recent years. With-out centralized management, each vehicle in VANET acts as both a wireless router and a network node to maintain the communication of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). Through the frequent interaction of real-time data on road conditions by wireless sensors, vehicles can obtain road conditions [3] like congestion, icing, accidents or other transport incidents in advance, so the safety of vehicles is well guaranteed. However, the great openness of VANET makes it more vulnerable to various attacks than traditional networks. For attackers outside VANET, security schemes based one ncryption and authentication can be a good solution.

Nevertheless, these defensive schemes have no effect on the attacks inside VANET. Attacks inside VANET can greatly impede data interaction between vehicles. Because messages between vehicles contain the key information of life safety, itis of great significance to identify malicious nodes in VANET so as to ensure the success of communication. To cope with the threat brought by malicious nodes inside VANET efficiently, reputation-based malicious node identification schemes have been proposed and gains ever-growing attention. The source nodes identify a node whether it is malicious based on its reputation and then choose a satisfying route for communication. Based on that, a series of work have been conducted: Wenjia Li et al. focus on the data trust and node trust simultaneously to identify malicious nodes; Chakeret al. propose a

solution based on the adaptive detection threshold to identify malicious behaviors. employ theTrusty Dynamic Software Agent (TDSA) to eliminate black hole attacks from VANET; Watchdog model is proposedto detect black hole attacks. ID-Based signature, Hash MessageAuthentication Code (HMAC) and RSA based algorithm[11] are used in the trust model to detect malice and integratemassages. study the influence on SAODV and ARAN caused by black hole attacks. Reputation-based schemes in and pay attention to the problem of slander and harboring.However, these methods still have many shortcomings and limitations, such as only effective for specific attack, high computational complexity and poor scalability. In conclusion, the existing schemes have the following major drawbacks:•Many methods like only take one specific at-tack behavior into account. Consequently, these methods are only effective for specific attack mode and lacking in good scalability.• Some researches such as attempt to secure the exchange of information based on cryptography, which contributes to the high cost in terms of computational complexity and mobility adaptation

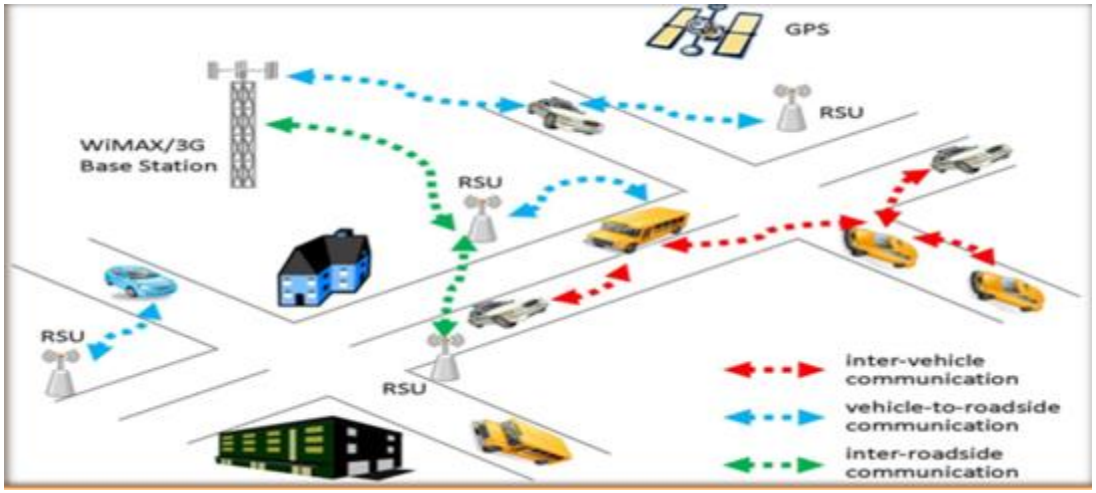
.•Schemes like MOO and FGT-OLSR calculate the reputation of nodes by combining direct and indirect reputation, but these methods ignore the feedback of communication results. This leads to the low efficiency and effectiveness.

VANETs in the Urban Environment

The vehicular ad-hoc network (VANET) is also called network on wheels, which is used to provide communication between vehicular nodes. It is an offshoot of mobile ad-hoc networks. In VANETs, vehicular nodes are self-organized and communicate with each other in aninfrastructureless environment . Knowing the importance of vehicular ad-hoc network for providing safety-related applications in Intelligent Transportation System (ITS), the IEEE committee has developed the IEEE 802.11p standard for VANETs [1]. The US Federal Communication Commission (FFC) department has assigned 75 MHz of bandwidth at 5.9 GHz for dedicated short-range communication (DSRC), which is used to provide communications between vehicle to vehicle and vehicle to infrastructure . The main aim of VANETs is to build an intelligent transportation system. DSRC can play an important role in building communications between vehicle to vehicle (V2V) and vehicle to infrastructure (V2I). The range of DSRC is about one thousand meters . From the last few years, inter-networking over VANETs has been achieving massive momentum. Realizing its intensifying significance, academia, major car manufacturers, and governmental institutes are

making efforts to develop VANETs. Various significant projects are initiated by different countries and famous industrial firms such as Daimler-Chrysler, Toyota, and BMW for inter-vehicular communications. Some of these prominent projects include CarTALK2000 , Car-to-Car Communication Consortium (C2CCC) [10], Advanced Driver Assistance Systems (ADASE2), California Partners for Advanced Transit and Highways (California PATH) , FleetNet , DEMO 2000 by Japan Automobile Research Institute (JSK) , Chauffeur in EU , and Crash Avoidance Metrics Partnership (CAMP) . These developments are a key step toward the recognition of intelligent transportation services.

The position-based routing protocols use the geographical position of source and destination to accomplish communication between them destination to accomplish communication between them. Every node is aware of its position due to global positioning system (GPS). The position of the neighboring node is found through beacons exchange. The position of the destination node is found using location services. When source node or intermediate node wants to send data to the destination node, if the destination node is in its transmission range than it directly forwards packet to the destination node. If the destination node is not in the transmission range it will forward the packet to a neighbor node that is the nearest to the destination node. In this way, the packet is relayed to destination [8,15–18]. In position-based routing, every node maintains one-hope neighbor information. Existing position-based routing protocols are developed for highway environment and urban environment. The highway environment consists of straight roads architecture without obstacles. On the other hand, urban environment consists of obstacles in the form of buildings. It is composed of streets and junctions. The points where two or more streets meet each other are called junctions. The data packets are routed towards destination through a set of junctions .The routing of data in an urban environment is challenging because of obstacles. In the existing literature, there are many position-based routing protocols proposed for V2V and V2I communications considering the urban environment.



The architecture of VANET in two separate environments is shown in Figure 1.

a) Infrastructure environment:

Many of the organizations in the network are permanently interconnected in the infrastructure environment. The agencies present manage all types of traffic and external services. Manufacturers, legal authorities, (trusted third party) TTP, service providers, and manufacturing processes all play a role in the infrastructure environment. VANET models sometimes provide legal authority Sari et al. (2015).

Despite the fact that each country's laws and regulations vary, there are two main tasks: vehicle registration and offence reporting. Any vehicle in the administrative region receives a license plate after it is manufactured. TTP is also a part of this ecosystem, providing services such as credential management and time stamping. In VANET, service providers are also taken into account. Location Based Services (LBS) Fuentes et al. (2010)are among the services available.

b) Adhoc environment:-

In this type of network, vehicles and RSUs communicate on a regular basis. All of the vehicle nodes in this setting have three separate devices: an On Board Unit (OBU), a series of sensors, and a Trusted Platform Module (TPM). V2V and V2I communication is done by OBUs. With the assistance of sensors, knowledge about the status that can be exchanged with other vehicle nodes is communicated and judged Fuentes et al. (2010) .This method of contact contributed to improved road safety. TPM, which is installed on cars, can be used to store user credentials and crash information Papadimitratoset al. (2006) .

Attacks on Denial of Service (DOS)

The attacker attacks the communication medium to trigger a channel jam in this attack. The channel will no longer be open to nodes, and they will be unable to reach itLa and Cavalli(2014) .The basic concept is to overburden the network with traffic, rendering the network and services inaccessible to legitimate nodes. The vehicle nodes and network infrastructure would be destroyed and overworked as a result of this.

The network would be unable to execute accurately, denying services to authentic nodes and performing other tasks that are irrelevant Hasbullahet al. (2010)Insiders and outsiders are also capable of attacking VANETs.

The main goal is to make the network inaccessible to legitimate users. This can be accomplished by flooding the control channel with a large number of irrelevant messages. A DoS attack has a significant impact on main resources such as bandwidth, CPU, and memory. Attackers can disrupt the network and launch a DoS attack by jamming channels, overloading servers, or falling packets.

The different stages of DoS attacks are listed below:-

A. Basic Level: Overwhelm the Node Resources:-

The attacker's main goal is to use the network's resources so that legitimate users can no longer use them. As a result, the vehicle nodes in the network are unable to perform all of the essential and appropriate activities, and information cannot be shared between them.

Case 1:

DoS attack in V2V Communication: In this scenario, the attacker sends out a warning message about an accident at a specific venue. The victim node, which is behind the attacker node, receives the post. However, the sender node will continue to send messages because its aim is to keep the attacked node occupied with the verification process rather than doing useful work.

Case 2:

DoS attack on V2R communication: In this case, the attacker targets the RSU (Road Side Unit), The RSU will be preoccupied with verification proofs and will not be able to assist the nodes in their contact efforts. The RSU will no longer be accessible to the network's vehicle nodes. Knowledge about human protection and lives will not be transmitted to network nodes, which can be dangerous in some cases Hasbullahet al. (2010).

A. Extended Level: - Jamming the Channel: - In this situation, the intruder jammed the communication channel, making it unavailable for all other nodes in the network to communicate.

• Case 1:

In this scenario, the intruder sends a high-frequency channel to jam communication between any vehicles at random. Due to this attack, vehicles in this domain will be unable to send or receive

messages. If they leave the attack domain, they can send and receive messages Hasbullahet al. (2010).

Case 2: Due to a jammed communication path, communication between the vehicles and the RSU is not possible in this case.

In this scenario, an attacker attacks the infrastructure to jam the channel, making it impossible to send or receive messages to/from the nodes and the RSU due to the inaccessible network Hasbullahet al. (2010).

I. Background

VANET is an infrastructure less architecture with various heterogeneous technologies used for wired and wireless communication to provide the intra-vehicle and inter-vehicle communication. Detailed overview of Architecture of VANET, Routing in VANET, Security Challenges and Applications of VANET discussed in the following subsections:

Table 2 Comparison of various proposed security schemes on VANET

Algorithm	Type of solution	Attack covered	Parameter	Tools	Remark
DOS attack-‘‘signature based authentication’’ in VANETs (Pooja et al. 2014)	Cryptography base (authentication using HMAC)	Inside and outside DOS	Authentication delay	NS-2.34	Not effective if the attacker floods the system with valid signature
Prevention of Sybil attack using ‘‘priority batch verification’’ (Kumar and Maheshwari 2014)	Encryption based	Sybil attack	Encryption time	No simulation	Provide security in a restricted manner
‘‘Trust-based scheme for alert spreading in VANET’’ (Ltifi et al. 2015)	Trust based (Cluster based trust management	False warning	Average delay	NS-3	This solution is totally based on vehicle cooperation

	system)				
ART:''attack-resistant trust management scheme'' (Li and Song 2016)	Trust based (trust calculation)	Simple attack, bad mouth attack	Precision, recall, communication overhead	GloMoSim 2.03	Calculate data and node trust, increases overhead
''Hierarchical and adaptive trust based solution for vehicular networks'' (Kerrache et al. 2016a,b)	Trust based solution based on three level architecture	Dishonest node detection	Detection ratio, end to end delay	NS-2	Complex and more overhead
Detection and prevention system against collaborative attacks (Khan et al. 2017)	Detection and prevention	Worm hole attack	Packet drop rate, false positive rate, detection time	NS-2	Increases the overhead on nodes, Limited to wormhole attack
''Adaptive trust and privacy management framework'' (Pham and Yeo 2018)	Trust and encryption based method	Internal and external attacks	Detection rate, trust linkability	ONE simulator	Framework address the trade-off between trust and privacy protection
Coupling of privacy and safety in VANETs (Wahid et al. 2019)	Pseudonym and encryption based	Syntactic/ semantic linking attack, Sybil attack etc.	Congestion confirmation delay, entropy of anonymity set	NS-2 and SUMO	Maximizes anonymity level of a moving vehicle as well as maintains the QoS of safety Applications

Algorithms for Detecting Existing Packets

A. Attacked Packet Detection Algorithm(APDA)

Every RSU is equipped with the APDA algorithm, which allows all vehicles to communicate with each other and with RSUs using only this algorithm. This algorithm aided in the identification of vehicle locations in the network.

After the location is detected, it is saved in an RSU for later usage. Devices such as OBU and TAMPERPROOF are installed on each vehicle and store detailed information such as speed and location. The OBU, frequency, and velocity of the vehicles actually aid in the identification of vehicle positions in the network.The algorithm can aid in the identification of malicious nodes by detecting malicious packets. The location saved in RSURoselinMaryet al.(2013) can be used to track down the malicious car.

B. Enhanced Attacked Packet Detection Algorithm(EAPDA)

RSU is used to communicate in this model, and control packets are used to communicate.The EAPDA algorithm was used by RSU to request and verify vehicles.Only vehicles that have been checked by RSU will be given services and network resources, while all nodes that are responsible for DoS attacks by flooding communication channels will be denied access to any network resources.This would improve the network's performance by increasing the availability of network resources to legitimate nodes.During the verification process, DoS attackers are identified.RSU calculates the time at which requests are sent and received, as well as the number of vehicles that send the request, in order to allot time slots to all nodes.

Vehicle id is used by the RSU to monitor a vehicle's future requests.In the time allocated.The number of packets being transmitted from each node will be analyzed by RSU.If a node's rate of sending packets exceeds a threshold value, it is considered malicious and must be removed from the network for successful communicationSingh and Sharma(2015).

C. Malicious and Irrelevant Packet Detection Algorithm(MIPDA)

This algorithm is an improved version of the APDA algorithm.It detects malicious nodes and packets based on frequency, velocity, speed, and road characteristics, just like APDA.Unlike APDA, it detects real packets by taking frequency and velocity values into account.This algorithm improves device security while reducing latency and overhead Quyoomet al. (2015)

Algorithm Proposed

This algorithm will aid networks in resisting DoS attacks, and if the network is attacked by malicious nodes, this algorithm will detect the malicious nodes and remove them from the network.packets that they send through the network.

As a result, this algorithm would aid in the continuous availability of the network for the dissemination of essential life-related knowledge.With the assistance of Road Side Units, this mechanism can aid in the identification of malicious nodes by detecting irrelevant packets (RSU).Each node will communicate with the RSU, allowing the RSU to save each vehicle's details.

Then, when a node sends harmful messages, the vehicle can be detected and tested using the information in RSU about its location.This algorithm is capable of detecting several malicious

nodes as well as the meaningless packets they send through the network.This algorithm belongs to the packet detection algorithm category.

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**

There are several nodes in the network. When multiple nodes in a network try to disseminate knowledge, they always communicate via RSU. RSU will examine the frequency and velocity of each node in the network and equate them to the upper and lower bounds of the threshold. If a node's freq and vel are greater than the prescribed range, the node is classified as malicious. Since those nodes are capable of launching DoS attacks, they must be isolated as soon as possible. The RSU keeps track of these nodes, both in terms of their location and the messages they send out into the network. Following their detection, these nodes are disconnected from the network and forbidden from sending any packets to legitimate users. The packets are useless and will not be forwarded in the network to legitimate users if the freq and vel are both big. Malicious nodes send these packets to jam the networks, which can result in a DoS attack at any time. If both the freq and the vel are tiny, these packets aren't from malicious nodes, but instead contain valuable information about the network node or the traffic ahead climate conditions As a result, all packets

with this configuration are forwarded to all nodes in the network. So, using the proposed algorithm, we can detect several malicious nodes and distinguish between nodes that send malicious and meaningless packets and nodes that send genuine packets in the network.

The following output parameters were used to evaluate this work:
a) Packet Loss: This is the ratio of packet loss to total packets sent to the destination by any node.Its value is determined by network congestion, which causes packets to fail to reach their destinationMokhtar and Azab (2015) Nethravathy and Maragatham (2016).

b) Network lifetime: A network's lifetime is described as the amount of time that its vehicles are able to successfully route data.

The network's lifespan ends if any amount of nodes run out of energy or lose functionality for any cause.

c) Network Throughput: The value of network throughput is the percentage of data sent from the originator node to the final node in a given amount of time.
The higher the throughput value, the more data is sent between the source and destination.

d) Packet Delivery Ratio: The value of the packet delivery ratio is determined by the accuracy with which packets are delivered from the originator to the destination.It's the ratio of the total number of packets to the number of packets reachedNethravathy and Maragatham (2016)

e) Dead and alive nodes: The number of nodes that stop operating is referred to as dead nodes, while the number of nodes that disseminate information throughout the network is referred to as alive nodes.
The simulation was completed entirely in NS-2. Since the network must deal with several nodes, the first simulation is carried out with just five nodes.

Fig. 2. Multiple nodes in simulation environment

Figure 2 shows the simulation screen in NS-2 which contains number of nodes in the network. All the nodes willcommunicate with each other by disseminating useful information through RSU. The network throughput is shown in Figure 3 which is measured n Gbps (Gigabits per second). and Figure 4 showsthe 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.

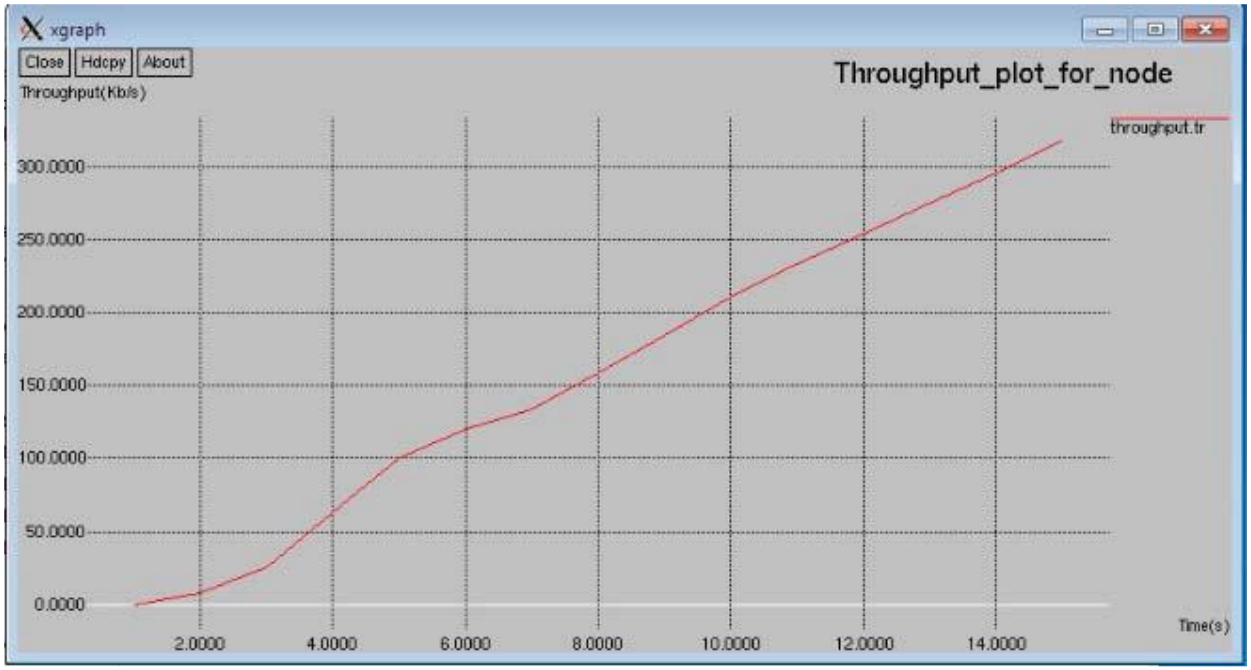


Fig. 3. Network Throughput with 5 nodes in network

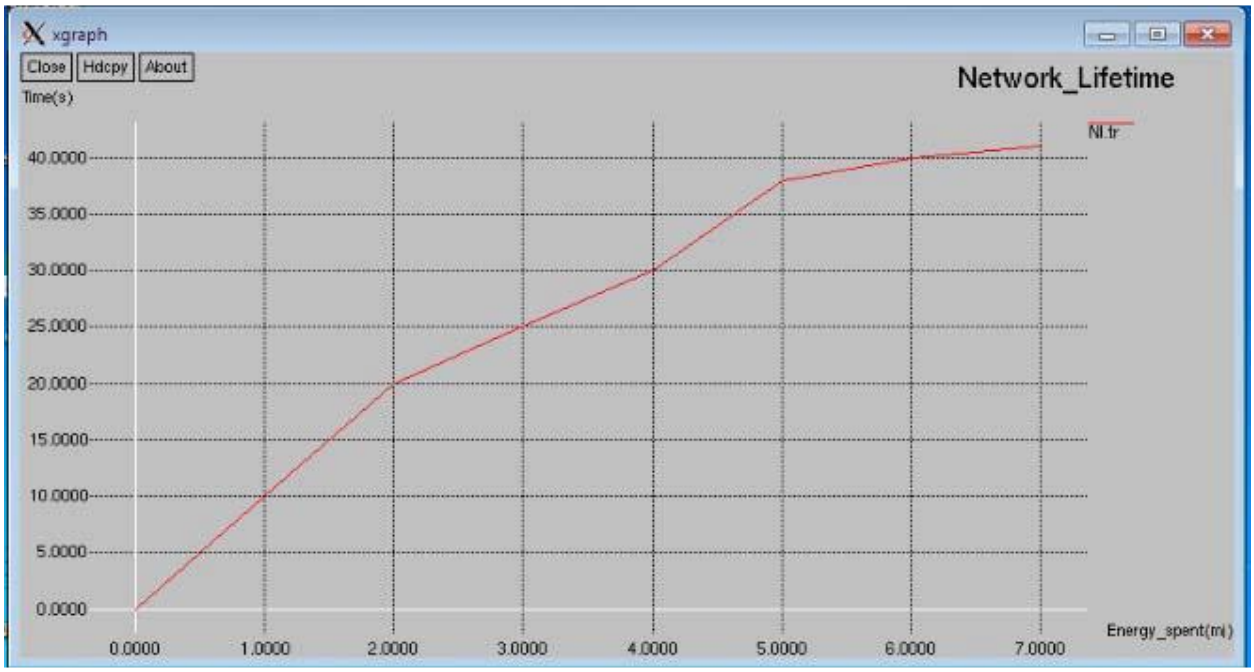


Fig. 4. Network Lifetime

The packet delivery ratio is shown in Figure 5. 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.

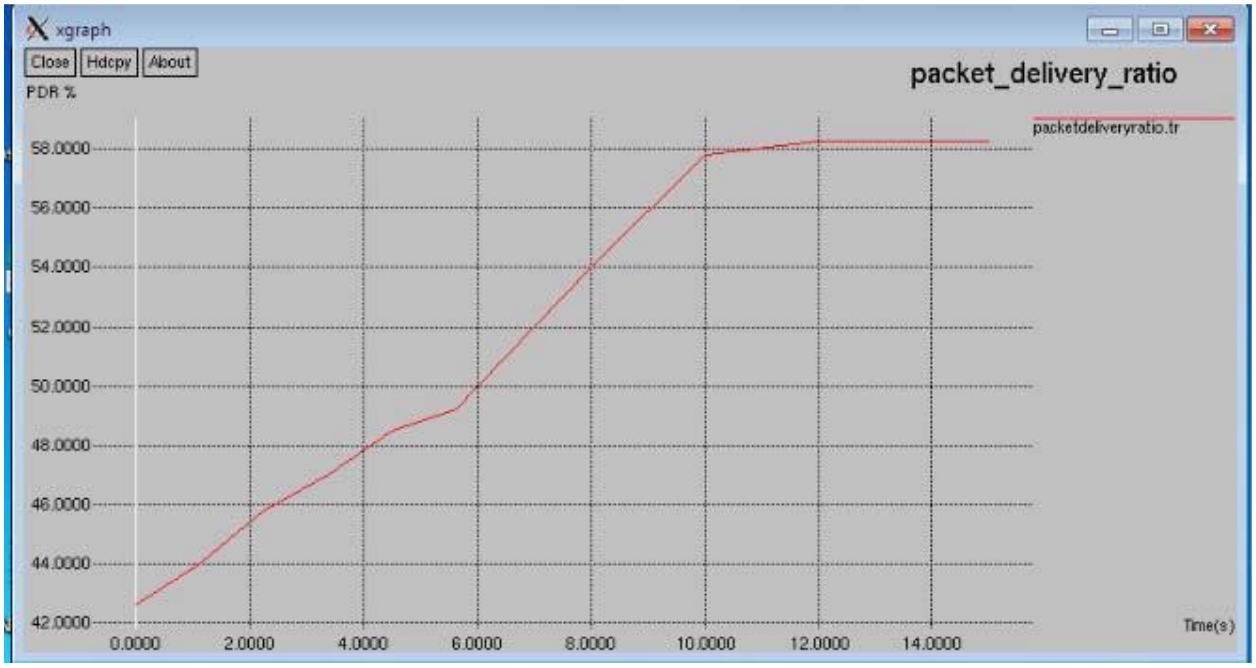


Fig. 5. Packet Delivery Ratio

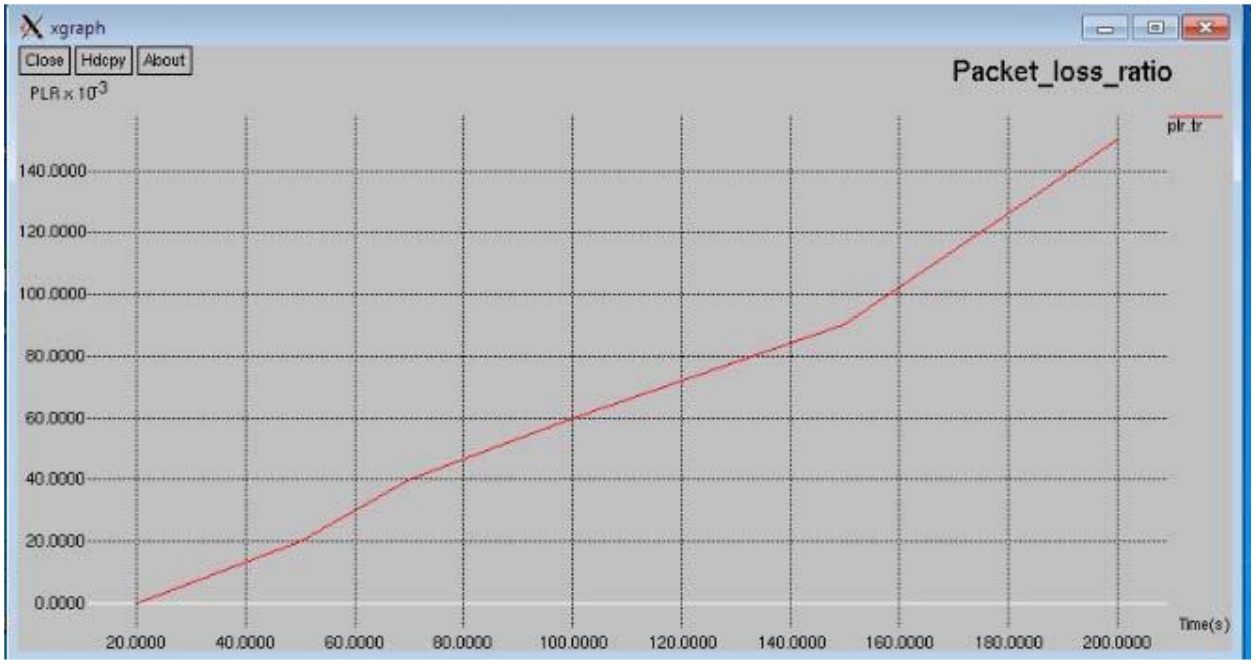


Fig. 6. Packet Loss Ratio

The proposed algorthm for detection of multiple malicious nodes is simulated using different number of nodesthat is taking 5, 8, 10 and 12 number of nodes. Figure7 shows the simulation of 12 nodes with multiple RSUs.

Figure7: Simulation with 12 nodes

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.

TABLE I: 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 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.

Conclusion

On the basis of frequency and velocity, the nodes responsible for attacking the network are described in this paper.This algorithm is capable of detecting both irrelevant and genuine packets.Unlike existing algorithms, which can only detect a single node attacking the network, the algorithm can detect multiple nodes attacking the network. The network's lifespan is extended by detecting intruder nodes in a timely manner. Other output parameters also indicate a significant difference in values, indicating that the proposed algorithm is a better version of current packet detection algorithms.

Reference

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

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.

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.

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.

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.

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.

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.

A. Quyoom, Ali, N. Gouttam , H Sharma ,“A Novel Mechanism ofDetection 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.

K.Thilak,”DoS attack in VANET Routing and possible defendingsolutions – a survey”, Proc in IntConf on Information Communicationand Embedded Systems, IEEE, 2016 doi10.1109/ICICES.2016.7518892.

J. Fuentes, A. Tablas, A. Ribagorda,”Overview of security issues inVehicular Adhoc Networks”, Handbook of Research on Mobility andComputing, IGI Global, 2010.

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

S. Zeadally, R. Hunt, Y. Chen,A. Irwin, A. Hassan,”VehicularAdhocNetworks (VANETs):status, results and challenges,”Springer Scienceand Business Media, LLC 2010, pp 217-241, doi 10.1007/s11235-010-9400-5.

A. Sari, O. Onursal, M.Akkaya, “Review of the Security Issues inVehicular Adhoc Networks (VANETs)” Int J. Communications, Network and System Sciences, 2015, Vol 8, pp 552-566, doi10.4236/ijcns.2015.813050.

A. Malla , R Sahu ., “Security Attacks with an effective solution for DoSattacks in VANETs” IJCA(0975-8887), Vol 66, No 22, March 2013, pp45-49.

B. Mokhtar, M. Azab, “Survey on Securiy Issues in Vehicular AdhocNetworks” Alexandria Engineering Journal, Science Direct, Vol. 54, Issue 4, December 2015, pp 1115-1126.

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

J. Nethravathy, G. Maragatham,”Identifying Malicious Nodes andPerformance Analysis in VANET” Int Journal of Applied EngineeringResearch, Vol. 11, No. 9 (2016), pp 6716-6719.

Arya KV, Tripathi KN (2013) Power aware and secure routing in mobile and ad-hoc networks. In: 2013 IEEE 8th international conference on industrial and information systems, pp 477–482 Bedi P, Jindal V (2014) Use of big data technology in vehicular ad-hoc networks. In: International conference on advances in computing, communications and informatics (ICACCI), pp 1677–1683

Eiza MH, Ni Q, Owens T, Min G (2013) Investigation of routing reliability of vehicular ad hoc networks. EURASIP J WirelCommunNetw 1(1):179.

Issariyakul T, Hossain E (2009) Introduction to network simulator 2 (NS2). In: Introduction to network simulator NS2. Springer, Boston, pp 1–18

Kerrache CA, Calafate CT, Lagraa N, Cano JC, Manzoni P (2016a) Hierarchical adaptive trust establishment solution for vehicular networks. In: 2016 IEEE 27th annual international symposium on personal, indoor, and mobile radio communications (PIMRC), pp 1–6

Kerrache CA, Lagraa N, Calafate CT, Lakas A (2016b) TFDD: a trust-based framework for reliable data delivery and DoS defense in VANETs. VehCommun 1(9):254–267.

Khan U, Agrawal S, Silakari S (2015) Detection of malicious nodes (DMN) in vehicular ad-hoc networks. ProcediaComputSci 1(46):965–972.

Khan FA, Imran M, Abbas H, Durad MH (2017) A detection and prevention system against collaborative attacks in mobile ad hoc networks. Future GenerComputSyst 1(68):416–427.

Krajzewicz D, Hertkorn G, Ro¨ssel C, Wagner P (2002) SUMO (simulation of urban mobility)—an open-source traffic simula-tion. In: Proceedings of the 4th middle east symposium on simulation and modelling (MESM20002), pp 183–187

Kumar N, Chilamkurti N (2014) Collaborative trust aware intelligent intrusion detection in VANETs. ComputElectrEng 40(6):1981–1996.

Kumar PV, Maheshwari M (2014) Prevention of Sybil attack and priority batch verification in VANETs. In: International confer-ence on information communication and embedded systems (ICICES 2014), pp 1–5.

Kumar V, Mishra S, Chand N (2013) Applications of VANETs: present & future. CommunNetw 5(01):12.

Li W, Song H (2016) ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks. IEEE Trans IntellTranspSyst 17(4):960–969.

Lim K, Manivannan D (2016) An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks. VehCommun 1(4):30–37.

Ltifi A, Zouinkhi A, Bouhlel MS (2015) Trust-based scheme for alert spreading in VANET. ProcediaComputSci 1(73):282–289.

Lu Z, Qu G, Liu Z (2018) A survey on recent advances in vehicular network security, trust, and privacy. IEEE Trans IntellTranspSyst 23(99):1–7.

Mokdad L, Ben-Othman J, Nguyen AT (2015) DJAVAN: detecting jamming attacks in vehicle ad hoc networks. Perform Eval 1(87):47–59.

Pham TN, Yeo CK (2018) Adaptive trust and privacy management framework for vehicular networks. VehCommun 13:1–2.

Pooja B, Pai MM, Pai RM, Ajam N, Mouzna J. (2014) Mitigation of insider and outsider DoS attack against signature based authen-tication in VANETs. In: 2014 Asia-Pacific conference on computer aided system engineering (APCASE), pp 152–157.

Saleh AI, Gamel SA, Abo-Al-Ez KM (2017) A reliable routing protocol for vehicular ad hoc networks. ComputElectrEng 1(64):473–495.

Sedjelmaci H, Senouci SM, Abu-Rgheff MA (2014) An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks. IEEE Internet Things J 1(6):570–577.

Sharma S, Chang V, Tim US, Wong J, Gadia S (2019) Cloud and IoT-based emerging services systems. Cluster Computing 22(1):71–91.

Singh A, Sharma P (2015) A novel mechanism for detecting DOS attack in VANET using enhanced attacked packet detection algorithm (EAPDA). In: 2015 2nd international conference on recent advances in engineering & computational sciences (RAECS), pp 1–5

Tyagi P, Dembla D (2016) Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET). Egypt Inform J 18(2):133–139.

Wahid A, Yasmeen H, Shah MA, Alam M, Shah SC (2019) Holistic approach for coupling privacy with safety in VANETs. ComputNetw 148:214–230.

Yao X, Zhang X, Ning H, Li P (2017) Using trust model to ensure reliable data acquisition in VANETs. Ad Hoc Netw 1(55):107–118.

Zaidi K, Milojevic MB, Rakocevic V, Nallanathan A, Rajarajan M (2016) Host-based intrusion detection for vanets: a statistical approach to rogue node detection. IEEE Trans VehTechnol 65(8):6703–6714