iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** XII **Month of publication:** December 2022

DOI: https://doi.org/10.22214/ijraset.2022.48249

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue XII Dec 2022- Available at www.ijraset.com

Detection and Prevention of Worm hole Attack to Improve Traffic in VANET

Annu Lakher[1], Mr. Rajneesh Pachouri[2], Mr. Anurag Jain[3]
[1, 2, 3]*Department of Computer Science and Engineering, RGPV, Bhopal*

Abstract: ***A Wireless Sensor Network (WSN) made up of spatially dispersed independent devices using sensors is vulnerable to many different types of threats and attacks due to a number of factors, including the unattended deployment in an untrusted environment, the limited network resources, the ease of network access, and the range of radio transmission. One of these weaknesses is the wormhole attack, in which a hacker sets up a low-latency link between sensor nodes in order to sabotage them, use up network resources, and steal sensitive information. This essay outlines the WSN wormhole attack and provides a critical assessment of the defences. Wireless sensor network defences against wormhole attacks and wormhole detection methods are contrasted and evaluated for their efficacy (WSN).***

Because there are unwanted attackers present, secure communication is absolutely necessary for the community. The bundle appears to be disintegrating, but most likely due to the attacker, according to the wormhole. If the intrusion is discovered in time, the perpetrator can be found and expelled from the network before any potentially dangerous actions are taken or data is corrupted. Similar to that, the suggested Worm hole serves as a deterrent and protects you. Information on entrance tactics that might be utilised to protect the access point can be found using the suggested device. The performance of the prior device, which is also the best and safest network to use, can be used to assess the correctness of the results. The packets connecting the nodes to the network can be used to calculate the agreement's cost.

Keywords: Worm Hole, VANET, MANET, Adaptive Cruise Control.

I. INTRODUCTION

Wireless ad hoc networks known as vehicle ad hoc networks (VANETs) connect moving objects to adjacent infrastructure. A new generation of wireless networking capabilities for autos is a developing technology. In addition to providing effective vehicle-to-vehicle communications that support Intelligent Transportation Systems, one of the main goals of VANET is to provide ubiquitous connectivity to mobile users who are already connected to the outside world through other networks at home or at work while they are on the go (ITS). Real-time route calculation, blind crossing (a crossing without controlled illumination), cooperative trac monitoring, trac ow control, and accident prevention are a few examples of ITS applications. There aren't enough methods for the metropolis's nearly 17 million residents to get there. One of the duties of being a member of this nation is to consider and attempt to resolve its problems [6].

Using NS2 as a simulator, a network layer attack is imitated (or "Worm Hole"). In a Worm Hole attack, a hostile node poses as the first hop on the shortest path in order to carry out a denial of service assault. A packet sent to a Worm Hole node is not forwarded to the next hop; instead, it is dropped. It is challenging to identify a node as a Worm Hole since so many trustworthy nodes in a VANET reject packets for valid reasons. VANET is a gureless topology. For this reason, the node(s) aren't stationary, hence a malicious node might roam around and pretend to be a reliable node. Worm Hole nodes must be blocked using the MAC address[6].

Vehicle ad networks (VANETs), a small subset of mobile ad networks, use vehicles as their nodes, such as cars, trucks, buses, and motorcycles (MANNETs). As a result, the nodes' ability to travel is constrained by elements like the direction of the road, which combines traffic with traffic laws. Due to the restricted node mobility, it is envisioned that VANET will be supported by a fixed infrastructure that offers a set of services and maybe access to static networks. Consistent infrastructure will be built in key locations such ice highways, gas stations, risky crossings, or areas that are particularly vulnerable to disastrous weather.

Although the concept of vehicular ad hoc networks (VANET) is not new, it consistently presents fresh research problems. A group of cars can develop and maintain a communication network among themselves with the aid of VANET without the need for a controller or a centralized base station. VANET is one of the most important uses in situations involving life-threatening medical emergency where there is no infrastructure but it is essential to relay information to save lives. These beneficial VANET applications do, however, also create additional issues and challenges.

Because of a lack of infrastructure, vehicles in VANET have new responsibilities. Every new vehicle that joins the network is in charge of and in charge of managing the network's connectivity as well as its own communication requirements. Occasionally, automotive ad hoc networks are used to handle communication between moving vehicles. Direct communication between two cars is known as vehicle-to-vehicle (V2V) communication. [5,6]. Vehicle-to-Infrastructure (V2I) communication refers to direct communication between a vehicle and an infrastructure, such as a Road Side Unit (RSU) (V2I). A representative VANET arrangement is shown in Figure 1.

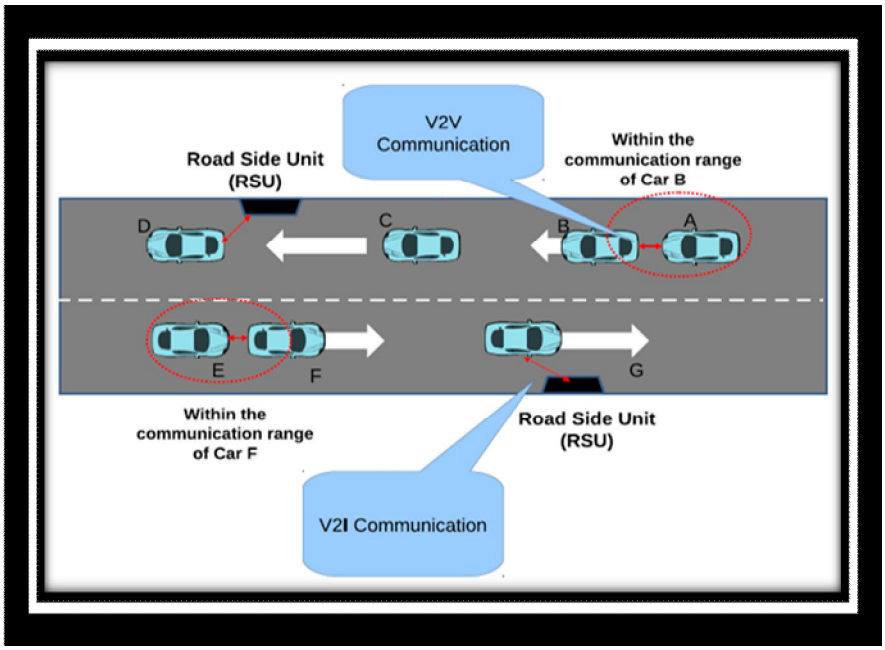


Figure 1Creating an Ad-hoc Network using Vehicles (VANETs)

II. RELATED WORK

"[27]Lingyun Zhu; Chen Chen; Xin Wang; Azman Osman Lim "SMSS: Symmetric-Masquerade Security Scheme for VANETs" Published in: 2011 Tenth International Symposium on Autonomous Decentralized Systems, 3-27 March 2011 Accession Number: 11929122, IEEE Xplore: 05 April 2011, DOI: 0.1109/ISADS.2011.88, ISBN:978-1-61284-213-4. "

Altogether, Lingyun Zhu [27] The Symmetric-Masquerade Security Scheme (SMSS), a ground-breaking security system that can meet security needs while remaining at the top of the system, is what we propose in this work. The emphasis of SMSS is on car-to-car interactions, which are among the most frequent occurrences on VANETs. Our method uses pre-allocated keys to provide authentication, local fake names to protect anonymity, and symmetric encryption to ensure message compatibility. The suggested programme develops a full description of the novel system before evaluating its performance in comparison to the PKI defensive system. This application uses fake names and encryption in place of the usual public/private encryption, which improves security for VANETs.

(1) Outstanding reduction in overprotection and computational speed, as well

(2) Effective privacy protection with pseudonyms. However, some important issues are needed to be resolved in order to achieve the full potential of this novel program, such as delivery technology.

For VANET The message must be verified and saved. The messages are conveyed in real-time, thus the packaging and counting time should both be as brief as is practical. The methods discussed in this article maintain message validation while also providing shorter calculation times and fewer packets. During RSU identification, quick hand-to-hand verification by fast automobiles is decreased, and inter-vehicle communication between various RSU units is improved. PKI security methods are inappropriate for VANET due to the communication's real-time and quick mobility.

With the aid of the road unit (RSU), message authentication to VANET is made simpler, but there are still certain problems, such as how to manually process the vehicle message within a different RSU communication and how to verify the authenticity of a message provided from a different RSU range. Due to traffic congestion, which causes unanticipated changes in network architecture, the effective and efficient dissemination of information is a significant difficulty. VANET is a very good place since the communication paradigm enables time, space, and synchronisation amongst connected enterprises.

The author suggests using our publishing and subscription model to disseminate knowledge on VANET.As a result, we have taken into account a hybrid VANET that consists of mobile and stationary information channels, each of which can serve as a publisher, registrar, or vendor. There are stationary information channels spread out around the metropolitan region that act as the last local authority for publications and subscriptions.

The effective and efficient dissemination of information is significantly hampered by traffic congestion, which results in unexpected changes in network design. Because the communication paradigm allows for time, distance, and synchronisation among connected businesses, VANET is a very good place. The author advises utilising our publication / subscription architecture to distribute material across VANET. In order to account for this, we have considered a hybrid VANET made up of mobile and stationary information channels, each of which can act as a publisher, registrar, or vendor. The metropolitan area has fixed information channels that serve as the final local authority for publications and subscriptions. These data cables, which are connected to the Internet, allegedly make up a Distributed Hash Table (DHT) merchant overlay. They serve as a central location for subscriptions and books and offer similar messages to prospective subscribers. These information channels also provide access to all vehicles on the network. The simulation results show that our technique operates most effectively when there are more vehicles available to boost its performance.

"[28]Gongjun Yan, Danda B.Rawat "Vehicle-to-vehicle connectivity analysis for vehicular ad-hoc networks", Received 6 July 2016, Revised 20 October 2016, Accepted 30 November 2016, Available online 10 December 2016, Version of Record 27 February 2017, Ad Hoc NetworksVolume 58, April 2017, Pages 25-35."

Danda B. Rahat and Gongjun Yan [28] The author offers a plan that addresses the problems of fuel waste and pollution. This is because many drivers leave their vehicles running as they wait for signals. By coupling the car to the traffic signal, we can ensure that the engine shuts off automatically.

A lot of factors influence how the engine stops. If certain requirements are satisfied and specific parameters are discovered, the engine will shut off. When one of these components is changed, the engine starts on its own, sparing the driver the effort of having to manually unlock the engine. There is an I2V connection used at the beginning of each junction line.The first group of route automobiles are informed when to expect the traffic light. These cars then transmit the information to their faulty vehicles over a V2V connection. I2V and V2V connectors should take into account a number of criteria when designing them, including width, bandwidth, direction, etc.

A set of flags is also required to keep track of the vehicle's status. These issues are looked at in the sections that follow. As a result, depending on the waiting time it has received and the condition of the flags, each car will automatically turn off its engine. One of the most exciting VANETs driving assistance systems is Vehicle Collision Warning Systems [28].The Distance Safety Warning, another element of these systems, warns the driver when they are approaching another vehicle. It can also apply emergency stops when the space between two cars or between a car and barriers unexpectedly narrows. Another application for these systems is when an accident has already occurred and nearby vehicles need to receive alerts (warning messages) to avoid mass collisions. In these situations, multihop communication can be used to disseminate collision information. For these applications to deliver a crucial safe driving system, localization systems must be robust, accurate, and dependable.

Vision Enhancement is a different driving aid that gives drivers a clear vision of cars and other obstacles in dense fog and the ability to find hidden cars, structures, and other vehicles. [28] combines the vehicle area measurement to assess and anticipate the risk of a collision at a road crossing and the Kalman filter to predict trajectory in an effort to increase road safety. The authors point out that even with unavoidable delays and setup errors, app performance is still satisfactory if the Kalman filter is used for prediction and measurement.

III.ROUTING PROTOCOLS

"The class of transitory networks known as VANETs are based on ad hoc router protocols that were first used in MANETs and tested for use in the VANET area. These address-based routes and topology must be assigned a unique address to each participating site. We therefore require a mechanism that may be applied to assign various addresses to various cars. These guidelines do not, however, guarantee that the network will not contain any duplicate addresses".

A. Routing Protocols Based on the Topology

These router protocols use the network data that is available on the network to deliver packets. They can also be divided into reactive (on-demand) and active (table-driven) routes.

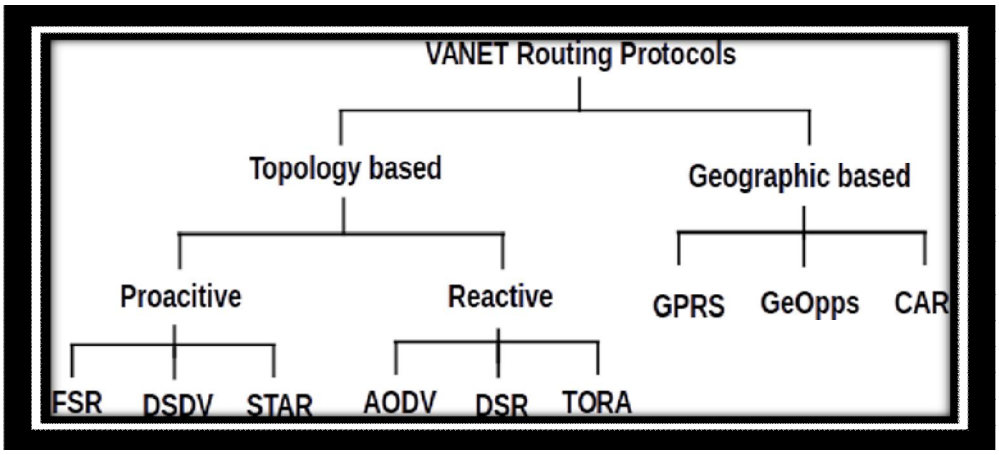


Figure 2 Routing Protocols of VANET

B. Active Route Protocols

Functional routing systems like Dynamic Source Routing (DSR) and Ad hoc On-demand Distance Vector (AODV) routes use route decisions on a case-by-case basis and maintain only used routes, reducing network load, when only a small number of routes are available for utilisation at any given moment. In a VANET system, when only a relatively limited number of pathways are used for vehicle communication, a functional route is extremely helpful.

Ad hoc On-Demand Distance Vector Routing (AODV) is a distance vector routing protocol that distributes routes over a directed and vector distance. Since each mobile host acts as a separate router and collects routes as needed, the network can start up by itself. Sequence numbers are used to regulate messages in order to prevent the "counting to infinity" issue that Bellman and Ford encountered and track loops.

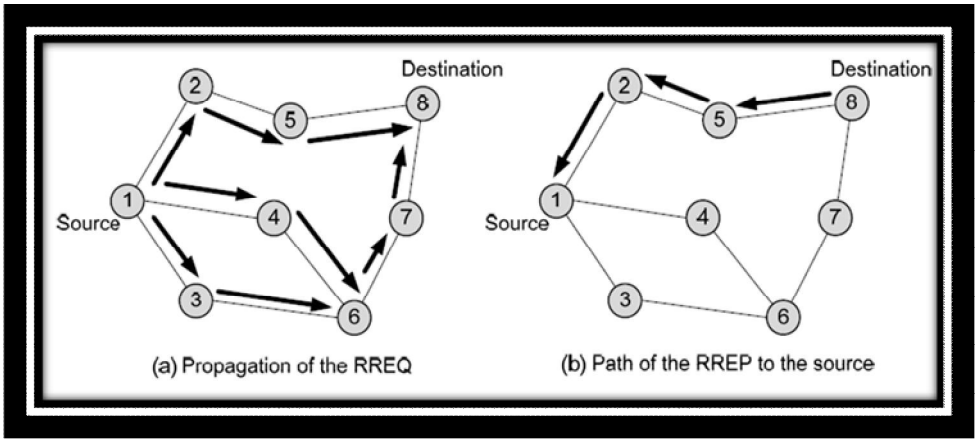


Figure 32 AODV Routing Procedure

In order to find a destination route, the node sends the RREQ (Route Request) message. Receiving nodes send the RREQ until it finds a new route (i.e., a route with a related serial number equal to or greater than the RREQ) to the destination or an intermediate point. Later, a location that leads to the RREQ source divides the RREP (Route Response) message.

Link breakages are signalled via RERR (Route Error) messages, which are sent to locations. Following the establishment of the path between the source and the destination, route maintenance is implemented to evaluate the route's usefulness because road nodes may move autonomously or close as a result of power outages. It includes a comparison of the two active Protocols and a feature summary.

IV. WORM HOLE ATTACK

Mobile Ad hoc Networks (MANETs) work without any kind of established infrastructure. For the purpose of sending data to its destination, each node in the network serves as a router. Because MANETs lack a centralized point of control, they are more vulnerable to routing assaults than traditional networks. Wormhole attack, one of the riskiest routing assaults, is straightforward to use but challenging to detect. Usually, the process happens in two steps: first, the wormhole nodes use the wormhole channel to draw a growing volume of traffic to themselves, and then, second, they begin to disrupt the network by modifying or deleting the content. Different writers for MANETs have proposed various defenses against wormhole attacks. In this study, we thoroughly evaluate different existing methods for wormhole attack detection in MANETs based on their strengths and weaknesses.

Due to the remarkable improvement in wireless communication technology over the past several years, Mobile Ad hoc Networks (MANETs) have evolved in a variety of ways. The key characteristics of MANETs include a lack of infrastructure, a shared broadcast channel, a dangerous wireless environment, the absence of a centralized point of control, a dynamic topology, and resource limitations. MANETs can be used for many different things, including obtaining useful information in disaster areas, enhancing soldier communication on the battlefield, and gathering and sending crucial information in the ocean, among other things. In a MANET, each node performs the roles of a host and a router, interacting directly with other nodes that are nearby and within its transmission range. With the help of other nodes in its neighborhood, a node builds an indirect link with non-neighbors hop by hop. Routing protocols are essential for finding, keeping up with, and fixing routes in the network. Researchers have proposed a number of routing protocols for MANETs during the past few years.

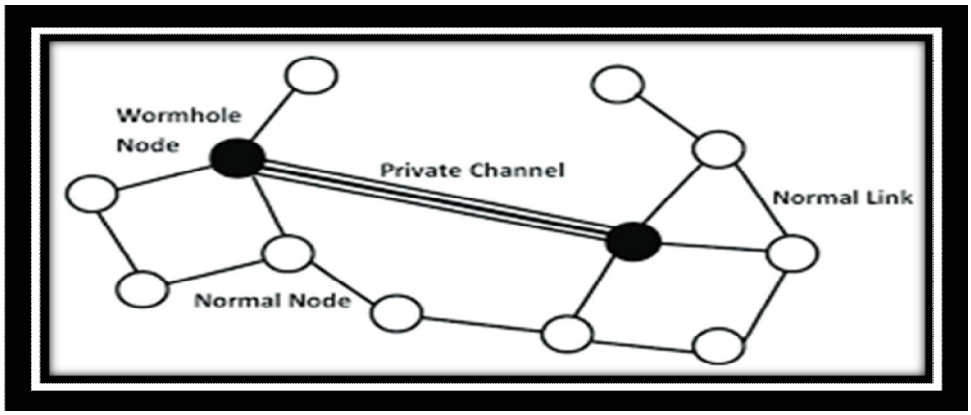


Figure 4 Wormhole Attack Working in MANETs.

Wormhole attacks are widely considered as one of the most significant security dangers to MANETs. Some MANET routing techniques, such as Topology Dissemination Based on Reverse-Path Forwarding (TBRPF), Ad hoc On-Demand Distance Vector (AODV), Optimized Link State Routing (OLSR), Destination Sequenced Distance Vector (DSDV), and Dynamic Source Routing, can be hampered by it (DSR). A wormhole attack is often conducted by two or more hostile nodes using a tunnel, a secure connection between them. Figure depicts a wormhole attack in action. A malevolent node at one end of the tunnel snoops on a control packet and sends it, over a private channel, to a helpful node at the other end, which then rebroadcasts the packet locally. When compared to packets carried over other conventional channels, the private channel has better metrics, such as fewer hops or less time, making it the preferred path for communication between the source and the destination. The attack typically has two phases. The initial stage involves the wormhole nodes taking a variety of routes. In the second step, these malicious nodes start using the packets they are given.

These nodes can hinder the network's functionality in a number of different ways. These nodes may deceive protocols that rely on node position or closeness to other nodes, for example, or they may cooperate to repeatedly transfer data packets back and forth across a virtual tunnel to drain the batteries of other intermediary nodes. Through wormhole nodes, data can be dropped, changed, or sent to a third party in order to harm someone else.

V. PROPOSED WORK

A. Worm Hole Attack Detection Method

1) A traffic monitoring system keeps track of activity along a chosen route.
2) The roadside unit is used to initialise the traffic monitoring system.
3) Ifk^{th}vehiclereceivesroute request andnot forward to next vehiclethen.
a) Traffic surveillance system Observe any suspicious vehicle activity.
b) If a suspicious vehicle makes a route request with a false Sequence Number, then
c) Traffic monitoring systems track suspicious vehicles' unusual behaviour.
d) If abnormal behavior detectsthen
e) This suspicious vehicle was identified as a worm hole vehicle by the traffic monitoring system.
f) Information is sent to the preventer node by the traffic monitoring system.

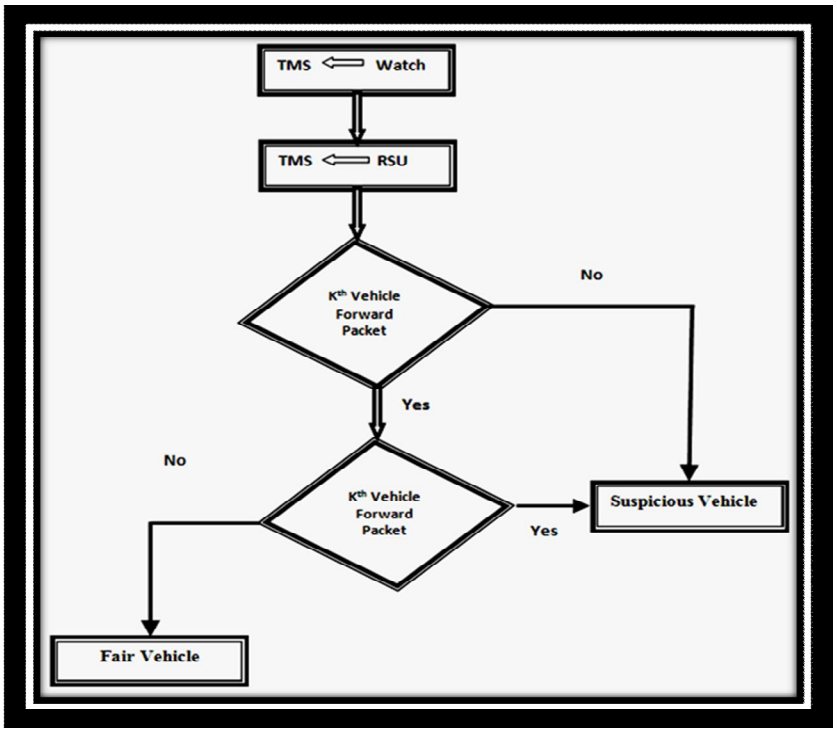


Figure 5 Worm Hoel Attack Detection Method

B. Worm Hole Attack Prevention Method

1) The response is obtained from the traffic monitoring system by the traffic preventer node.
2) The activity of suspect nodes is again examined by the traffic preventer node.
3) Traffic preventer nodes check hope count, capture packet, drop packet, and sequence number if a suspect vehicle exhibits wormhole behaviour.
4) If all these fields are abnormal of that vehicle, then Traffic preventer node take confirmation that vehicle is worm hole and block route from this vehicle.
5) The network-wide traffic monitoring system aired this vehicle's negative response.
6) Create a new route and restart it to accept these questionable vehicles.

C. Prevention Scheme

Security Scheme is used to identify the prevention process from malicious vehicles. Because the malicious vehicles are not chosen on a secure path, reliability also rises.

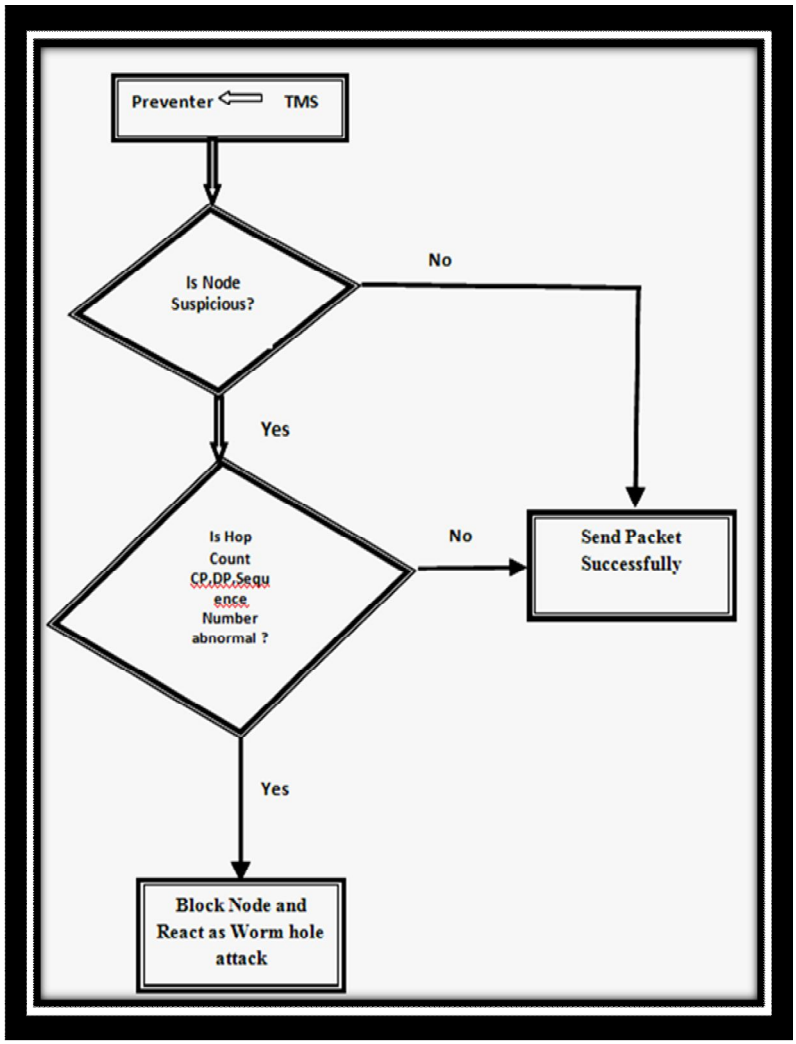


Figure 6 Worm Hole Attack Prevention Method

VI. RESULTS ANALYSIS

In order to assess the overall effectiveness of the suggested security system with DSR routing protocol, worm hole AODV and previous M-AODV are utilised (BAODV). There are nodes in many different contexts in every module. The recommended safety approach is performing better overall, as can be shown.

A. Throughput Performance Analysis

In automotive networks, throughput, often referred to as network throughput, describes the speed at which a message travels via a communication channel to the destination vehicle. Adding this information through a logical or physical link or avoiding it by using a specific network device are also options. Although it is often reported in bits per second (bit/s or bps), the throughput can also be expressed in statistics packets per time slot or facts packets per second. evaluating the throughput performance of the proposed Worm hole AODV, relaxed AODV, and secure DSR (DSR).If a hostile device enters the network and starts delivering records, the outcome could get worse, but if we utilise the BUS-AODV technique while the attack is taking place, throughput performance is once again better.

The throughput of the black hollow node in the community at the time of the performance reduction in all node density scenarios is very low. Although the suggested solution also improves performance, M-performance AODV's recovers the network's total performance.

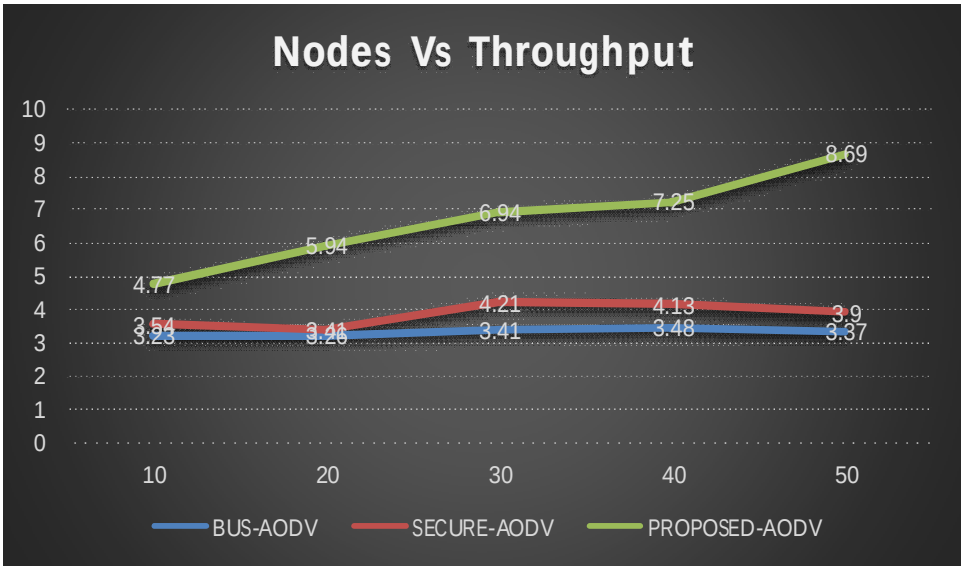


Figure 7Throughput Analysis

B. Packet Drop Performance Analysis

As a result of attacker negligence, a substantial percentage of traffic status packets are lost in the network. The VANET is particularly dependent on the routing protocol's availability because vehicles constantly transmit and receive traffic data to promote safer driving conditions. The only instance of a data drop in this graph is the existence of BAODV, BUS-AODV, and BUS -AODV. In this case, the attacker is deleting roughly 22500 data packets from the incoming traffic on the network. Due to the attacker's incorrect behaviour, which caused data packets to be missed, the vehicles are engaged with retransmitting the request, which results in the loss of this data. Data loss was decreased in comparison to the older security M-AODV system, and safe SDR implementation satisfied the security criteria for reliable communication. When there are 40 and 50 nodes, it is obvious that there is significant data loss.

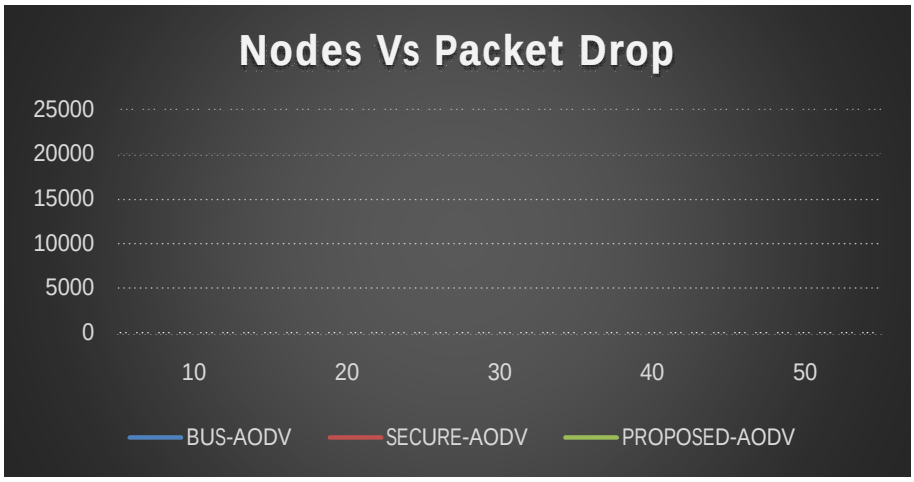


Figure 8 Packet Drop Analysis

C. PDR Performance Analysis

Proper communication is necessary in a network, but it is critical in a real-time traffic system. The inaccurate information provided by the trailing vehicles has caused the traffic on the road to VANET only transmits brief updates to cars close (about road conditions and unforeseen incidents like accidents).

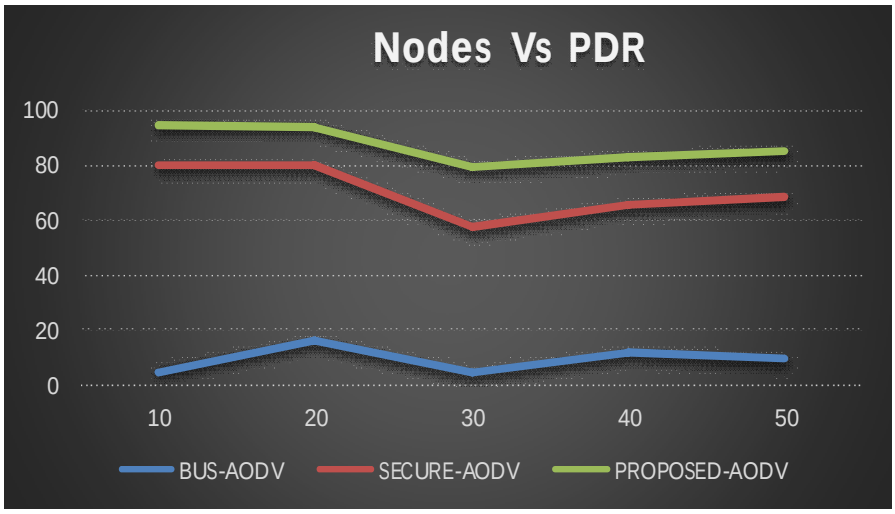


Figure 9 PDR Analysis

D. Packet Receiving Performance Analysis

VANET is utilised for communication in order to fulfil the needs of sender cars and maintain the flow of traffic on the roadways. In this graph, BAODV data receiving is small in comparison to SADV and M-AODV. If we adopt the suggested M-AODV with high data reception, worm hole attack cases lead to the maximum data loss, which is observed in all node density scenarios. The network gets contaminated as a result of this evidence that receiving from rogue nodes is genuinely irrelevant between the source and the destination. The suggested technique, however, results in improved performance, implying superior receiving to M-AODV. The data packets from the vehicle's attacker slow down the network's actual performance.

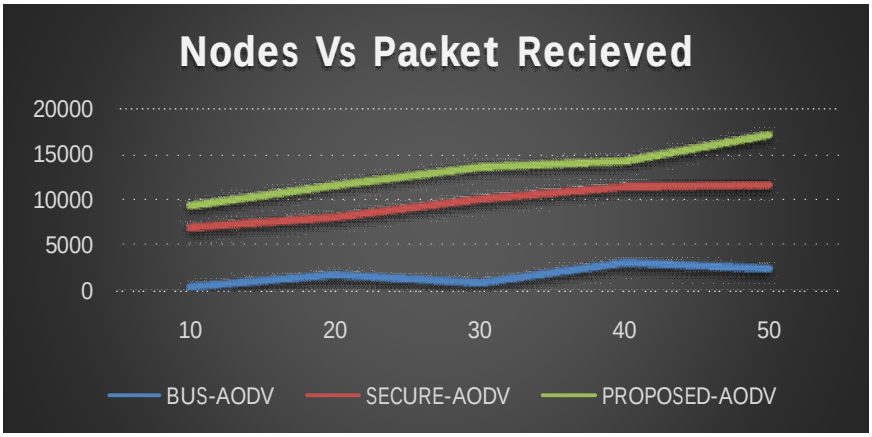


Figure 10 Packets Receiving Analysis

E. Delay Performance Analysis

The number of cars on the road is rising, and inaccurate information is being delivered to moving vehicles, which are the main causes of traffic delays. To monitor traffic flow, the following vehicles continuously transmit traffic requests. Based on the traffic data from the initial vehicles, the automobiles are driven along that route. If a network receives traffic information and responds improperly as a result of the presence of a Worm hole attacker, it could be hazardous (BAODV). The delay performance of BAODV, which is consistently high in all node density scenarios, is shown in this graph.

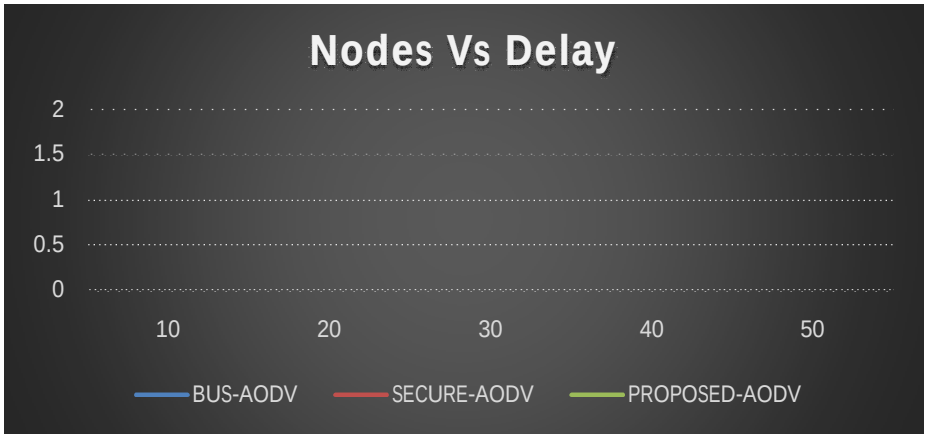


Figure 11 Analysis of Delay

The delay performance of BAODV, which is consistently high in all node density scenarios, is shown in this graph. The proposed M-AODV approach only uses a little amount of delay improvement. The suggested security measure assures that the network performance is secure and that request packet delivery is completed as rapidly as it would be on a typical VANET. Worm hole attackers can be prevented.

VII. CONCLUSION & FUTURE WORK

A defence against VANET wormhole assaults is recommended by this study. Wormhole assaults are the most dangerous since they can also lead to further attacks like sinkhole assaults, which cause sinkholes in networks by forging route information, and DOS assaults, which cause a persistent denial of service by sending packets into wormholes. The introduction of decision packets dramatically reduces the likelihood of the wormhole. Furthermore, the nodes do not require the installation of any new hardware.

The presence of malevolent vehicles unquestionably reduces the effectiveness of Attacker packet drooping is exacerbated in the presence of black holes, and transmitting and receiving are noticeably reduced in contrast to regular communication. The M-AODV security solution that is being suggested in this study is designed to identify and protect the network from VANET worm hole attacks that employ both a single and multiple worm holes. If the number of dropped packets rises above a predetermined threshold, the suggested method presupposes the presence of an attacker in the network. Terminals like RSU units are being used by cars more frequently.

In this paper, the AODV routing protocol was modified to detect wormhole assaults. The enhanced protocol is known as improved efficient routing protocol (IMAODV). The two primary elements of the IMAODV protocol are the RTT function and the clustering procedure. The hop-by-hop routing load is calculated by the RTT function during the communication process. Profits from RTT are anticipated to be used to establish clusters. The cluster determined the values of the diseased and normal nodes. It has been enhanced and replaced with the AODV protocol. The RTT and clustering method is a useful approach for wormhole discovery. This method will eventually be used for real-time wormhole identification.

REFRENCES

[1] Liang, W., Li, Z., Zhang, H., Wang, S., & Bie, R. (2015). Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends. International Journal of Distributed Sensor Networks, 2015, 17.

[2] Sumra, Irshad Ahmed, Iftikhar Ahmad, Halabi Hasbullah, and J-L. bin Ab Manan. "Classes of Attacks in VANET." IEEE Saudi International Electronics, Communications and Photonics Conference (SIECPC), 2011, pp. 1-5, 2011.

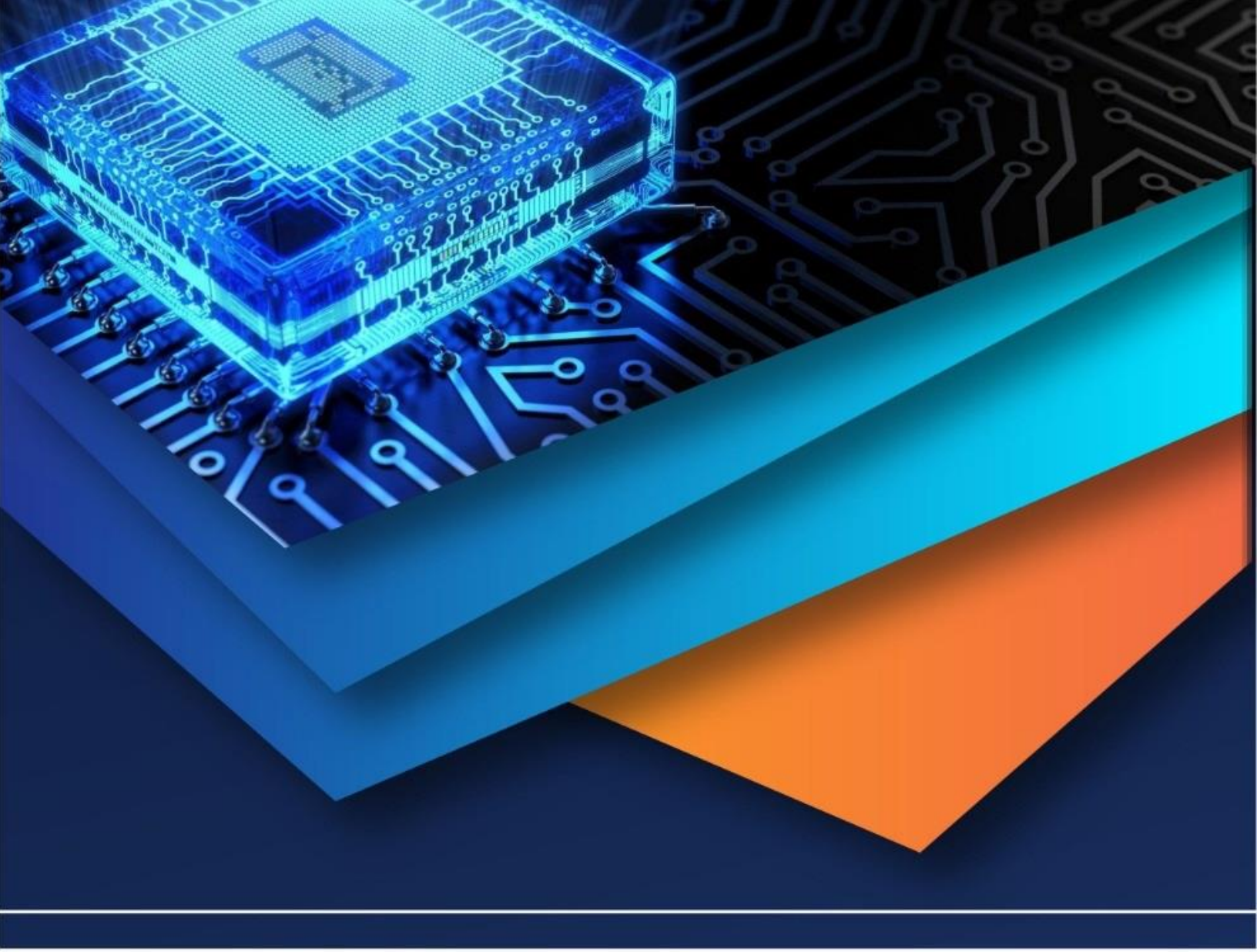
[3] Sarah Madi, Hend Al-Qamzi, "A Survey on Realistic Mobility Models for Vehicular Ad Hoc Networks (VANETs)", IEEE 10th IEEE International Conference On Networking, Sensing And Control (ICNSC), 2013.

[4] Vishal Kumar, Shailendra Mishra, Narottam Chand "Applications of VANETs: Present & Future", Communications and Network, 2013, 5, 12-15 doi:10.4236/cn.2013.51B004 Published Online February 2013.

[5] Mengjiong Qian, Yong Li, Depeng Jin, Lieguang Zeng", Characterizing the Connectivity of Large Scale Vehicular Ad-Hoc Networks", IEEE Wireless Communications and Networking Conference (WCNC): Networks, 2013.

[6] Sabih ur Rehman*, M. Arif Khan, Tanveer A. Zia, Lihong Zheng "Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges", Journal of Wireless Networking and Communications 2013, 3(3): 29-38

[7] Willke, T. L., Tientrakool, P., & Maxemchuk, N. F. (2009). A survey of inter-vehicle communication protocols and their applications. Communications Surveys & Tutorials, IEEE, 11(2), 3-20.
[8] Vishal Kumar, Shailendra Mishra, Narottam Chand "Applications of VANETs: Present & Future", Communications and Network, 2013, 5, 12-15 doi:10.4236/cn.2013.51B004 Published Online February 2013.
[9] Jair Jose Ferronato, Marco Antonio, Sandini Trentin, "Analysis of Routing Protocols OLSR, AODV and ZRP in Real Urban Vehicular Scenario with Density Variation", IEEE Latin America Transactions Volume: 15 , Issue: 9, pp.1727 - 1734, 2017.
[10] A.P. Jadhao, Dr.D.N.Chaudhari, "Security Aware Routing Scheme In Vehicular Adhoc Network", IEEE Proceedings of the Second International Conference on Inventive Systems and Control (ICISC 2018), 2018.
[11] Kumud Dixit Priya Pathak Sandeep Gupta, "A New Technique for Trust Computation and Routing in VANET", IEEE, 2016.
[12] Trupil Limbasiya, Debasis Das, "Secure Message Transmission Algorithm for Vehicle to Vehicle (V2V) Communication", IEEE, 2016.
[13] Khaoula Jeffane, and Khalil Ibrahimi, "Detection and Identification of Attacks in Vehicular Ad-Hoc Network", IEEE, 2016.
[14] Mengjiong Qian, Yong Li, Depeng Jin, Lieguang Zeng, "Characterizing the Connectivity of Large Scale Vehicular Ad-Hoc Networks", IEEE Wireless Communications and Networking Conference (WCNC): NETWORKS, 2013.
[15] Sourav Kumar Bhoi, Rajendra Prasad Nayak, Debasis Dash and Jyoti Prakash Rout, "RRP: A Robust Routing Protocol for Vehicular Ad Hoc Network against Hole Generation Attack ", International conference on Communication and Signal Processing, pp. 1175-1179 April 3-5, 2013
[16] M. Sivasakthi and S. Suresh, "Research on vehicular ad hoc networks (VANETs): an overview," Journal of Applied Sciences and Engineering Research, vol. 2, no. 1, pp. 23–27, 2013.
[17] F. Li and Y. Wang, "Routing in vehicular ad hoc networks MANETs: a survey," IEEE Vehicular Technology Magazine, vol. 2, no. 2, pp. 12–22, 2007.
[18] K. Hong, J. B. Kennedy, V. Rai and K. P. Laberteaux. Evaluation of Multi-Channel Schemes for Vehicular Safety Communications. In Proc. of IEEE VTC-Spring, Taipei, pp. 1-5, 2010
[19] H. Moustafa and Y. Zhang, Vehicular Networks: Techniques, Standards, and Applications, CRC Press, Boca Raton, Fla, USA, 2009.
[20] A. Amoroso, G. Marfia and M. Roccetti. Going Realistic and Optimal: A Distributed Multi-Hop Broadcast Algorithm for Vehicular Safety. Computer Networks, 55(10), pp. 2504-2519, 2011.
[21] J. Misic, G. Badawy and V. Misic. Performance Characterization for IEEE 802.11p Network with Single Channel Devices. IEEE Transactions on Vehicular Technology, 68(4), pp. 1775-1789, 2011.
[22] Y. Zhang, Q. Wang, S. Leng, and H. Fu. A QoS Supported Multi-channel MAC for Vehicular Ad Hoc Networks. In Proc. of IEEE VTC-Spring, Budapest, pp. 1-5, 2011.
[23] D. Jiang and L. Delgrossi. IEEE 1609.4 DSRC Multi-Channel Operations and Its Implications on Vehicle Safety Communications. In Proc. of IEEE VNC, Tokyio, pp. 1-8, 2009.
[24] Marc Torrent-Moreno, Daniel Jiang, Jannes Hartenstein "Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc networks" VANET '04: Proceedings of the 1st ACM international workshop on Vehicular ad hoc networksOctober 2004 Pages 10–18https://doi.org/10.1145/1023875.1023878
[25] S. Wang and C.-C. Lin. NCTUns 5.0: a network simulator for IEEE 802.11(p) and 1609 wireless vehicular network researches. In Proc. of IEEE VTC-Fall, Calgary, 11(2), pp. 3-20, 2008.
[26] T. L. Willke, P. Tientrakool and N. F. Maxemchuk. A Survey of Inter-Vehicle Communication Protocols and Their Applications. IEEE Communications on Surveys and Tutorials, 11(2), pp. 3-20, 2009
[27] Lingyun Zhu; Chen Chen; Xin Wang; Azman Osman Lim "SMSS: Symmetric-Masquerade Security Scheme for VANETs" Published in: 2011 Tenth International Symposium on Autonomous Decentralized Systems, 3-27 March 2011 Accession Number: 11929122, IEEE Xplore: 05 April 2011, DOI: 0.1109/ISADS.2011.88, ISBN:978-1-61284-213-4.
[28] Gongjun Yan, Danda B.Rawat "Vehicle-to-vehicle connectivity analysis for vehicular ad-hoc networks", Received 6 July 2016, Revised 20 October 2016, Accepted 30 November 2016, Available online 10 December 2016, Version of Record 27 February 2017, Ad Hoc Networks Volume 58, April 2017, Pages 25-35.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY