Enhance Security by using IDS Node in VANET to Improve Traffic Against DDos Attack

Ms. Richa Kori[1], Dr. Navdeep Kaur Saluja[2], Mr. Sarvesh Singh Rai[3]
[1] *Research Scholar, Department of CSE, IMEC, Sagar (M.P.)*
[2,3]*Associate Professor, Department of CSE, IMEC, Sagar (M.P.)*

***Abstract*—The primary concerns of every wireless network are security and safety. When the designated network is the Vehicle Adhoc Network (VANET), the issue is more serious. VANET is vulnerable to Distributed Denial of Service (DDoS) attacks, in which several vehicles launch different kinds of DoS attempts to prevent the network from operating normally and consequently jeopardize human life. The development of a highly effective and dependable algorithm is necessary to identify and stop DDoS attacks in VANETs. on order to detect DDoS attacks on VANETs, this study provides a hybrid detection technique based on the SVM kernel methods of AnovaDot and RBFDot. Features like packet drops, jitters, collisions, etc. are included in this hybrid method. The existence of uninvited attackers makes the need for safe communication an essential component of society. According to M-AODV, the bundle is collapsing, but it is doing so in a simpler way because the attacker is there. If access is identified quickly enough, the offender can be identified and taken off the network before any sensitive data or potentially harmful interests are tainted. In a similar vein, the suggested M-AODVacts as a wall, preventing intrusion. The suggested device makes it possible to gather data regarding entry tactics that could be applied to strengthen the entry point. The previous device's total performance makes it the best and safest network for determining value dependability and agreeable cost computation based on packets that connect nodes to the network. Performance measures are used to measure the overall performance of the proposed M-AODV, and the outcome shows an improvement in overall performance.**

***Index Terms*—M-AODV,Balckhole ,VANET , MANET , Adaptive Cruise Control.**

I. INTRODUCTION

The characteristic that sets vehicular ad hoc networks (VANETs) apart from mobile ad hoc networks (MANETs) is that their nodes are automobiles, such as cars, trucks, buses, and motorbikes. This suggests that node movement is constrained by elements such as road course, which includes traffic and traffic laws. It is reasonable to assume that the VANET will be supported by some fixed infrastructure that can give access to stationary networks and help with certain services due to the restricted movement of nodes. The fixed infrastructure will be installed at key areas such as service stations, slip roads, hazardous intersections, and areas with a history of bad weather.

Vehicular Ad hoc Network is abbreviated as VANET [1]. A unique class of Mobile Ad-Hoc Networks (MANETs) known as Vehicular Ad-Hoc Networks (VANETs) is made up of nodes that distribute information and self-organize. They are made up of automobiles and/or roadside apparatuses that provide network management. As VANETs are developed, security becomes increasingly crucial in system architecture. Security methods require additional concerns, such as privacy, authentication, and message consistency, due to the unreliability of VANET communications. However, due to the high communication overhead associated with earlier approaches, efficiency has hitherto been disregarded. Numerous methods for detecting intrusions in vehicular ad hoc networks (VANETs) have been presented. Other approaches, however, do not take into account the non-moving fake cars and the vehicles with a believable mobility model. We see the Vehicular Ad-hoc Network in Fig. 1

The term "vehicular ad hoc network" (VANET) refers to a network of moving cars that communicate independently and asynchronously. A significant obstacle to effective and scalable information distribution is vehicle movement, which can result in erratic changes to network architecture.

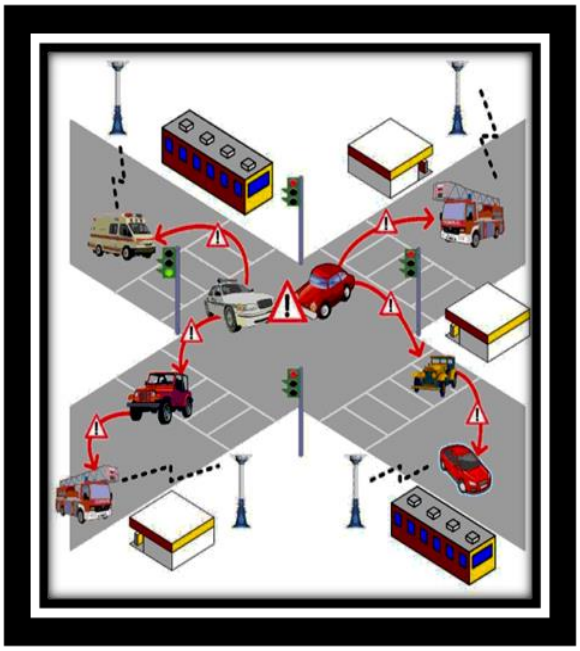

Figure 1 Vehicular Ad-hoc network

A. Vanet Application

The DSRC lists more than a hundred VANET programs that are advised. There are two types of these applications: those related to safety and those not. They can also be divided into applications that are OBU-to-OBU or OBU-to-RSU. A few of these uses are listed below:

- Co-operative Collision Warning
- Lane Change Warning
- Intersection Collision Warning
- Work Zone Warning
- Electronic Toll Collection (ETC)
- Parking Lot Payment
- Traffic Management

II. LITERATURE SURVEY

Sourav Kumar Bhoi et.al [1] Due to worries about traffic safety, the Vehicular Ad-hoc Network (VANET) focuses on the automotive sector. Network access should always be available since it is crucial when a node provides any crucial health information to other nodes. Security is another security aspect in VANET. The growth of wireless apps being created and disseminated in a well-known wireless environment, however, makes it likely that security threats will expand in the future. As a result, network access is vulnerable to several kinds of attacks. An introduction to a Distributed Denial of Service (DDOS) attack on network access is made in this study. The complexity of this attack's brutality in the VANET domain is discussed. The VANET paradigm has been used to prevent DDOS assaults developed and other possible solutions for overcoming attacks have been discussed.

Irshad Ahemed Sumra et.al [2] proposes five distinct attack stages, with each class being intended to offer a deeper understanding of VANETsecurity. The division and identification of various attacks on VANET are addressed in this paper's main contribution.

Hend Al-Qamzi et.al [3] accelerates data flow between vehicles and between roadside vehicles and traffic availability by integrating mobile communication devices. On VANET, messages can be sent from one automobile to another and the wireless device can broadcast information to neighbouring vehicles. Therefore, employing VANET can improve traffic efficiency and security. There are serious issues with VANET, just like with other technologies. Security is among the things that are most significant to them. One of the most crucial topics in the vehicle industry is safety, so I try to address it in this essay.

Jakub Jakubiak and Yevgeni Koucheryavy, al [4] is developing a crosslayer control system with an increased focus on vehicle tracking precision rather than MAC efficiency. The authors take into account a lost shared channel where an increase in message frequency can clog the channel and inadvertently reduce the accuracy of other vehicles' placements. With the help of the suggested algorithm, full accuracy can be attained by modifying the transmission periodicity.

Mengjiong Qian [5] The rate of packet injection is adjusted to achieve the desired channel load in the suggested approach for managing congestion. The issue of acquisition performance and choosing a full channel capacity is not, however, explicitly taken into account.

One of the most frequent security attacks on MANETs and VANETs is the black hole attack. When nodes decline to join a network or when a fixed node collapses, a black hole is produced. This kind of attack causes no data loss because all network traffic is diverted to a single point [5]. There are two potential remedies for this issue in MANETs. The

protocol finds several ways to get you there. It is obvious that the network could get very cluttered as a result of this method. Additionally, while this strategy might work for MANETs, adding another mobile node to a VANET with several mobile nodes would introduce needless restrictions like delays or service fees. The second solution is to use a package sequence number attached to any packet head [6].

Other methods [5] [6] [7] have recommended distributing information to VANET as settings using the publishing / subscription model. These techniques have been crucial in determining how effective VANET's publishing and registration are. In these systems, a mixed set is used to discuss a collaborative approach, including moving vehicles and stationary information stations. The ultimate objective is to create automobile networks' P/S middleware that accounts for the location and time of its design objectives. By using location as context, this middleware enables app developers to quickly broadcast a notification locally. It makes use of the possibility to produce subscriptions using data that may be derived from automobile navigation systems (location, map, driver location, etc.). The navigation system determines whether the vehicle wants to receive a specific notification or not. The proposed system is a program that takes advantage of Publish / Subscribe opportunities.

In this study [8] In order to analyse the placement and timing of radio transmissions, we present a novel model of congestion for urban transportation networks. We view the marked intersections and connected road segments as the fundamental elements of urban traffic systems in order to portray traffic congestion. The congestion model gives us a framework for characterising crucial radio frequency and local circuits in accordance with VANET scenarios intended for urban transportation systems, which is not possible with the same congestion models that are frequently employed in existing literature. In order to send a message of security to VANETs, it studies the channel volume associated with sporadic lighting using a remote radio model. This study also offers a common framework for analysis that can be used to look at further elements of data performance and security message transmission on VANETs. In order to reduce channel loading caused by crowded traffic circumstances, test findings utilising the suggested real-time congestion model point to the need for an adaptive strategy to modifying the transmission capacity and data level.

III. METHODOLOGY

A. Problem Identification

Due to its extremely dynamic nature, a VANET is vulnerable to both internal and external adversaries, posing significant technical hurdles for secure routing and dependability. Attacker driving patterns are more likely to result in routing misbehavior and are less sustainable and economical to implement than road construction methods.

The existence of Blackhole attackers in the network is the reason of the hostile conduct. Without a security guarantee, some misbehaving or malevolent cars weaken the system by offering subpar services or even putting the user cars in risky circumstances. As a result, identifying those misbehaving or malicious cars has emerged as a crucial need for VANET security. Malicious user vehicles can exhibit erratic behavior.

The ability of an attacker to create false information on a network and remove every traffic packet from the network. Due to packet losses in the network, the attacker vehicles increase network overhead. Retransmission of packets increases network latency as well, but ultimately, because of Blackhole presence, vehicle communication cannot be secured and traffic status cannot be accurately delivered. The proposed SDSR detects and stops hostile vehicles, enabling safe multi-hop data packet transmission.

B. Proposed Attack Identification and Removal Scheme

The suggested defense plan for VANET against a blackhole attack. Here, the Blackhole attacker is causing "gaps of information delivery" between cars, which slows down the pace of the vehicles and affects how well regular vehicles perform. In order to preserve security, the suggested strategy is implemented with V to RSU communication, forwarding the information about the attacker vehicle to all other RSU and the surrounding vehicles. The suggested preventative plan offers safe VANET communication while blocking the nefarious activities of the attacker. The actions listed below can be used to locate malicious cars within a network:

In order to provide destination vehicles with traffic status information, the sender cars deliver packets containing that information.

1) The number of sending vehicles are sending the traffic status to destination vehicles and the *attacker or malicious node presence is drop traffic information*. This is the behavior of attacker.
2) The whole research is divided in to three different scenarios.

i) To evaluate performance of only AODV protocol
ii) Evaluate Existing protocol performance of SAODV.
iii) Evaluate performance in presence of Validate Data Delivery Security Scheme with DSR.

3) Count the data receiving at the destination end in each scenario.
4) The counting of traffic status packets in case of attacker is minimum or negligible at destination end.
5) The presence of attacker is confirming but *which node is attacker.*

i) Check the receiving and forwarding of each node.
ii) if receiving is *true* and forwarding is *false* is found in routing table record then the attacker is found.
iii) Count the number of packets received by attacker but not forwarded.
iv) Otherwise, node is normal.

C. Flow Chart of Attacker Detection

The planned security scheme's flow chart illustrates the procedures for spotting an attacker's malevolent activity within a VANET. To determine which nodes in the network are consistently dropping packets, detection is necessary.

The Security Scheme is represented as the flow chart for preventing malevolent vehicles. Because the malicious cars are not chosen along a secure path, reliability also rises.

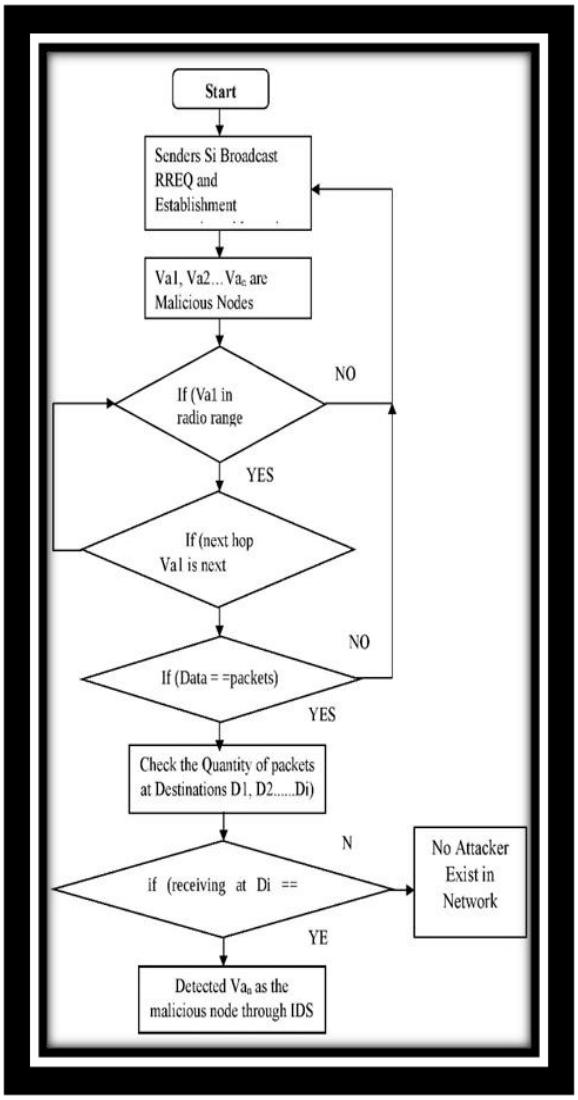

Figure 2 Flow Chart

IV. RESULTS ANALYSIS

NS2 (Network Simulator 2) [17] from Berkeley is an open-source event-driven simulator specifically designed for research in computer networks communication and applications. The simulator we have used to creating the network environment for the ad-hoc routing protocols. To simulate the mobile wireless radio environment, we have used a mobility extension to ns that is developed by the CMU Monarch project at Carnegie Mellon University. Since its inception in 1989, NS2 has continuously gained tremendous interest from industry, academia, and government. On the basis of simulation parameters given in Table 1 simulation has been done in ns-2 simulator (version 2.31).

A. Simulation Parameters

The simulation has to be done on the basis of Simulation parameters that are shown in table 6.1. The number of nodes is taken into account as mobile detector nodes. All node has random mobility speed to move in network. The simulator version is employed for simulation is NS-2.31[16]. The final parameters of Network parameters are listed in Table 1.

Table 1Simulation Parameters

NS-2.31	
Number of nodes	10, 20, 30, 40, 50
Attacker	Blackhole
Propagation	Two-Ray Ground
Antenna	Omi-directional
Dimension of simulated area	800×800
Routing Protocol	AODV
Performance Evaluated	BAODV, SAODV, SDSR
Simulation time (seconds)	100
Transmission Range (meters)	550
Transport Layer	TCP, UDP

The performance of proposed security scheme with DSR routing protocol is measured with previous SAODV and Black hole AODV(BAODV). The number of nodes scenarios is same in all modules. The performance of proposed security scheme is showing the better performance.

B. Throughput Performance Analysis

In Vehicular networks, throughput or network throughput is the successful message delivery over a communication channel up to destination vehicle. This data may be delivered over a physical or logical link, or pass through a certain vehicle in the network. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot. In this graph we compare the throughput performance of Blackhole AODV (BAODV), Secure AODV (SAODV) and proposed Secure DSR (DSR).

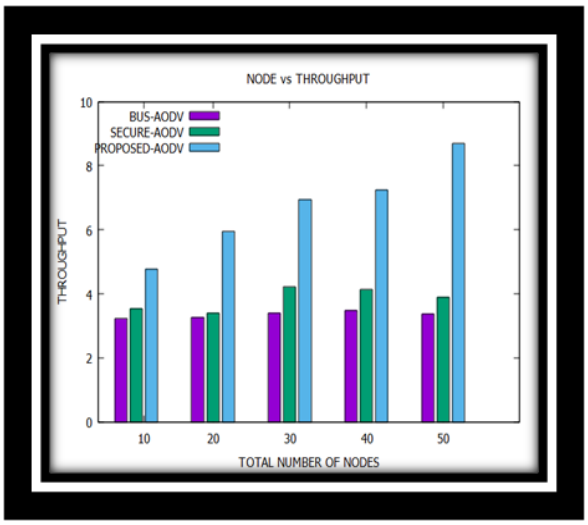

Figure 3 Node Vs Throughput

C. Packet Drop Performance Analysis

The number of traffic status packets are drop in network because of attacker misbehavior. The routing protocol existence is also important in VANET and the vehicles are continuously sends and receive traffic data in network for better driving facility on roads. In this graph only data drop in presence of BAODV, SAODV and SDSR is evaluated. Here the assailant presence is dropping about 22500 packets of data in network of total data of traffic is receives in network.

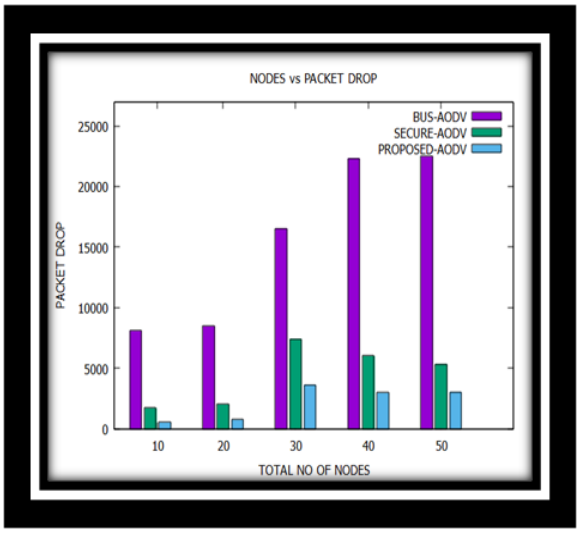

Figure 4 Node Vs Packet Drop

D. PDR Performance Analysis

The proper communication is necessary in network but it is very important in real time traffic system.

The vehicles wrong information is misguiding the trailing vehicles and because of that the road traffic is In VANET only short information (about traffic status and something un-happened on roads like accidents) are deliver to nearby vehicles. In this graph the PDR performance of BAODV, SAODV proposed SDSR communication is assessed and observe that the proposed scheme is really effective to identified the Blackhole assailant presence. The PDR performance as compare to SAODV is better and provides 97% successful delivery at destination.

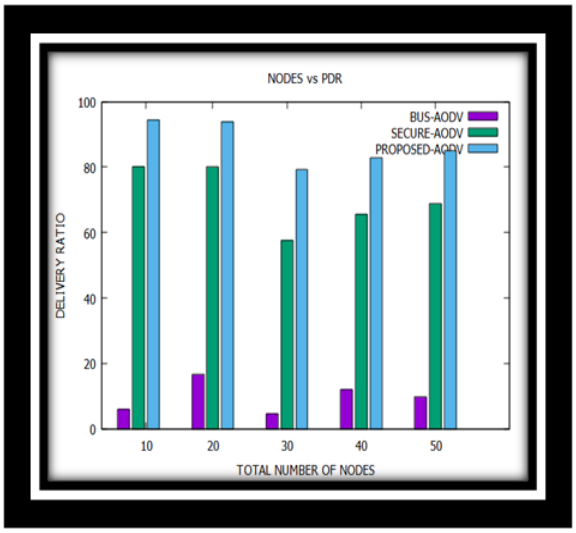

Figure 5 Nodes Vs PDR

E. Packet Receiving Performance Analysis

The communication is VANET complete the request of sender vehicles and maintain the traffic in roads. In this graph BAODV data receiving is negligible as compare to SADV and SDSR. that means black hole attack case data loss is maximum and if we apply proposed SDSR with data receiving is high, that shows in all node density scenarios. That shows receiving in case of malicious nodes is really insignificant in between source to destination that conclude network under the infection. The attacker vehicle consumes the data packets in network and decrease the actual performance of the network but in proposed scheme performance is increases means that shows better receiving as compare to SAODV.

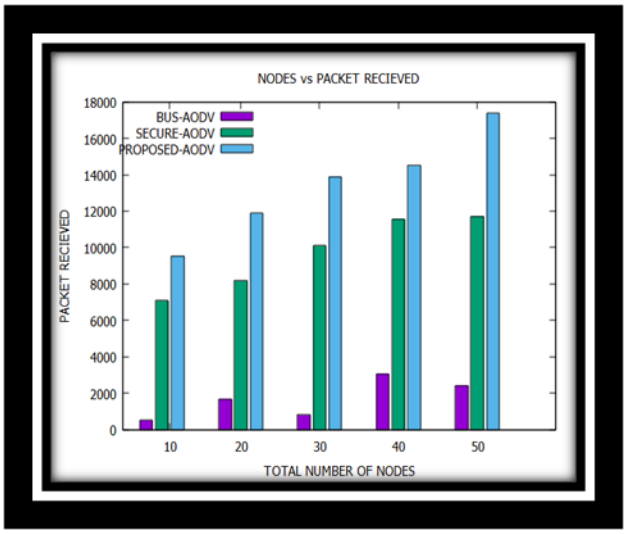

Figure 6 Nodes Vs Packet Receiving

F. Delay Performance Analysis

The delay reason in road traffic is vehicles in road is more and the traffic status information is nor delivered to vehicles properly. The follower vehicles are continuously sending the traffic request for recognizes the traffic status. The vehicles are drive on that path according to the traffic information of beginning vehicles. Traffic information is also destructive if it will be delivered in network e.g. perform misbehave due to presence of by Blackhole attacker (BAODV).

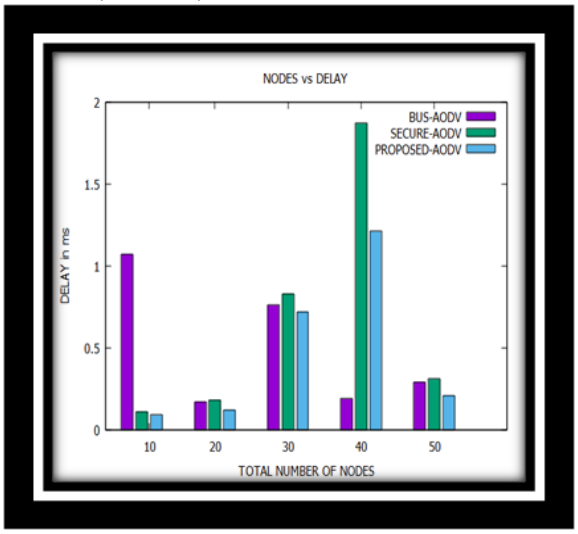

Figure 7 Nodes Vs Delay

V. CONCLUSION & FUTURE WORK

The presence of a malicious vehicle or vehicles significantly reduces the performance of the

network. In this research, the proposed SDSR security scheme is intended to detect and prevent the network from both single and multiple blackhole attacks in VANET. The suggested approach determines that if the number of packets drops exceeds a predetermined threshold, then the attacker may be present in the network. The number of vehicles that cross roads and terminals such as RSU units. The RSU unit is observe the traffic status information sending by the vehicles in limited range to identified the further traffic status from leading vehicles. In order to determine the current traffic state from leading cars, the RSU unit monitors the traffic status information sent by the vehicles within a specified range. The goal of RSU monitoring is to first identify the presence of the attacker and then stop it. Many aspects of VANET, including its environment, standards, and network architecture, have been discussed in this study

REFERENCES

[1] Sourav Kumar Bhoi, Eabitra Mohan Khilar, "A Secure Routing Protocol for Vehicular Ad Hoc Network to Provide ITS Services", International conference on Communication and Signal Processing, April 3-5, 2013.

[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] Jakub Jakubiak and Yevgeni Koucheryavy, "State of the Art and Research Challengies for VANETs", Proceedings of the 5th annual IEEE CCNC, pp.912-916, 2008.\

[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] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET Security Surveys," Computer Communication, Vol. 44, pp. 1–13, May 2014.

[7] Anas Abu Taleb, "VANET Routing Protocols and Architectures: An Overview", Journal of Computer Science, 2018.

[8] Duduku, V., V.A. Chekima, F. Wong and J.A. Dargham, "A Survey on Routing Protocols in Vehicular Ad Hoc Networks", International Journal Innovative Research of Computer Communication Engineering, pp.12071-12079, 2015.

[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.