International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 08 | Aug 2022 www.irjet.net p-ISSN: 2395-0072

M-AODV Routing Protocol in VANET to Detect and Prevent Black Hole Attack

Ms. Shubhvardhani Jain [1], Mr. Nilesh Kumar Sen [2]

M.Tech Research Scholar Department of Computer Science Engineering BTIRT, Sagar
Assistant Professor, Department of Computer Science Engineering BTIRT, Sagar

---

Abstract - *Due to the availability of additional attackers, the need for secure communication is an absolutely essential aspect of the community. According to M-AODV, the collapse of the bundle is primarily caused by the attacker's presence. If access is discovered quickly enough, the offender can be identified and disconnected from the network before any potentially dangerous interest or corrupted data can occur. The suggested M-AODV functions similarly as a barrier, protecting you from intrusion. The suggested device enables the gathering of data regarding entry tactics that may be applied to strengthen the access point. The previous device's overall performance is the best and safest network to determine the accuracy of the values, and the determination of the agreement cost depends on the packets that connect the nodes to the network. The efficacy of the suggested M-AODV prevention techniques as well as the presence of Blackhole attacks (BAODV), OldPrevention (M-AODV), and the efficacy of the same old direction are assessed. The receiver then recognises the droppings, sets the autumn limit, and recognises the presence of the attacker inside the system, which represents the attacker effect and also influences the performance of the network router. As a result, the performance of the proposed defence system is higher. The proposed M-AODV overall performance is measured by way of performance metrics and the result displays overall performance improvement.*

***Key Words*:-** M-AODV ,Balckhole ,VANET , MANET , Adaptive Cruise Control.

1. INTRODUCTION

The term "vehicle ad networks" (VANETs) refers to a tiny subset of mobile ad networks (MANNETs) whose nodes are automobiles, trucks, buses, and motorbikes. This means that factors like the road's route, which combines traffic with traffic laws, have an impact on how the nodes can move. It is assumed that VANET resolve to the supported by a fixed infrastructure that assists specific services and may enable access to static networks due to the restricted node mobility. Critical sites, such as slick roads, service stations, risky intersections, or regions that are particularly susceptible to hazardous weather, will be dispersed with consistent infrastructure. It is possible to imagine the Vehicular Ad-hoc Network (VANET) as a network of moving vehicles that interact in a non-autonomous way. Due to traffic congestion, which causes unexpected changes in system topology, the effective and efficient dissemination of information is put to the test. People who live in wealthy nations may struggle daily with traffic congestion. Road traffic conditions also have an impact on public safety because it is estimated that 1.2 million people die on the world's highways each year. Due to this, governments and the car industry are putting more money into improving road efficiency and safety while also lowering the environmental impact of transportation. A wide range of opportunities have emerged as a result of the usage of communication technology and information for this purpose. One of the most promising areas for research is communication between vehicles and sidewalk units, or especially current Vehicular Ad-hoc Net-work (VANET) traffic.

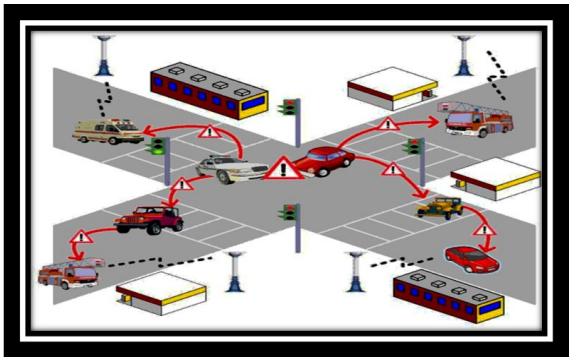

Figure 1 Vehicular Ad-hoc network

The DSRC lists more than 100 VANET programmes that it recommends. These safety and security-related applications fall under multiple categories. They can also be divided into OBU-to-RSU or OBU-to-OBU applications. Listed below are a few of the applications:

2. ROUTING PROTOCOLS

VANETs are a type of ad hoc router protocols that were developed for usage in MANETs and evaluated for use in the VANET space. It is necessary to assign a unique address to each participating site in order to use these address-based routes and topology. As a result, we need a system that may be used to give various addresses to distinct cars. However, these rules do not ensure that there won't be any duplicate addresses on the network. [3, 4]

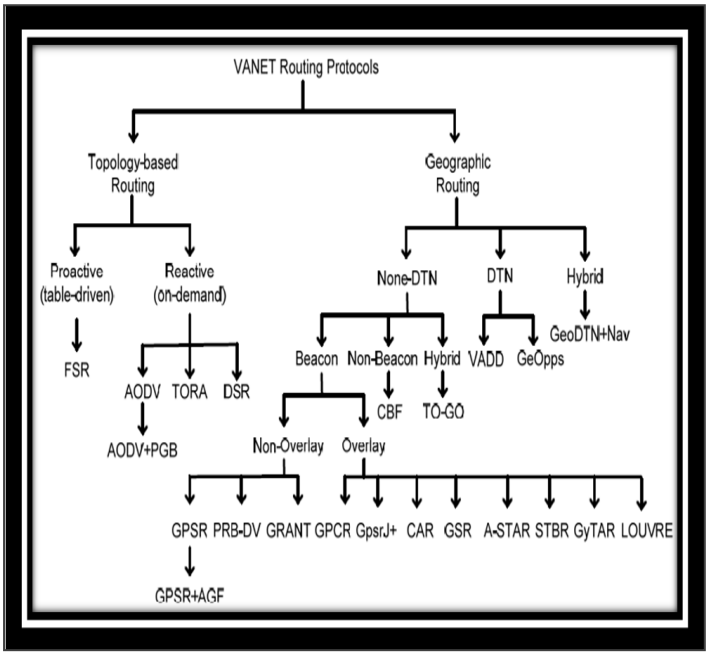

Figure 2 Various Routing Protocols in VANET

Figure 2 shows the VANET tax for these routes, which are classed according to topology and nation (based on geography). As a result, the speech algorithms now utilised in mobile ad networks are less appropriate in the VANET space. When a single data packet is sent to its destination, the most recent unicast router protocols are discussed in this section.

a. Topology-based Routing Protocols: - These router protocols transport packets using the network data that is accessible on the network. Additionally, they can be separated into active (table-driven) and reactive (on-demand) routes.

b. Active route protocols

Functional routing systems such as Dynamic When only a small number of routes are available for usage at any given time, Source Routing (DSR) and Ad hoc On-demand Distance Vector (AODV) routes use route decisions on a case-by-case basis and maintain just used routes, lowering network load. A functional route is especially useful in the case of a vanet system because the communication between vehicles will only employ a very small number of paths. A vectorrouting distance protocol, AODV (Ad hoc On-demand Distance Vector Routing) distributes routes as a directed and vector distance. The network can start up by itself thanks to the specific routing functions performed by each mobile host in the system. To avoid the Bellman-Ford problem of "counting to infinity" and track loops, sequence numbers are used to control messages.

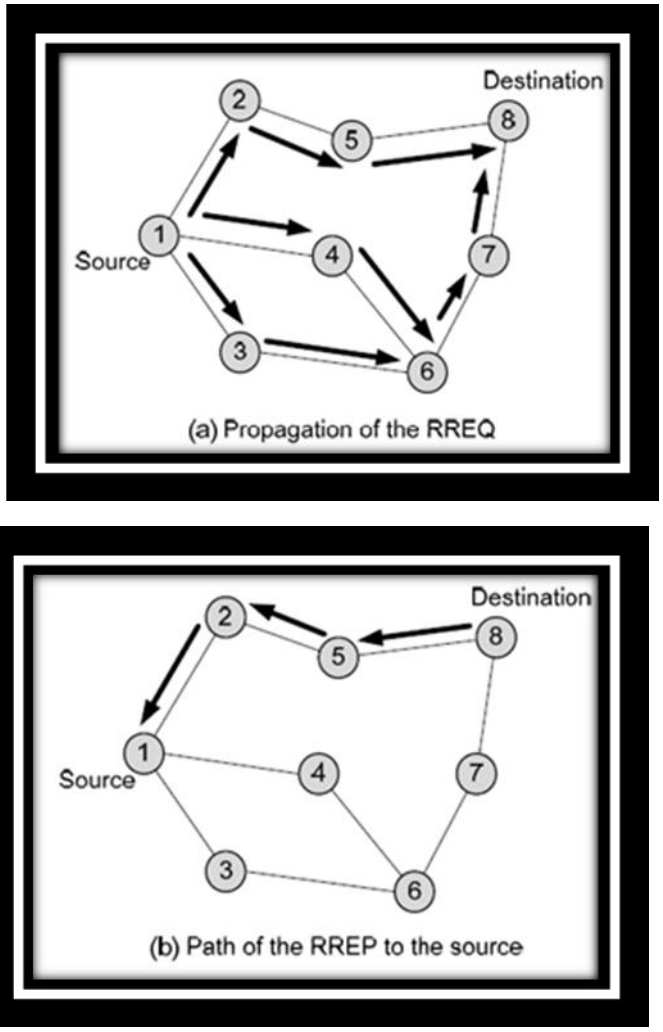

Figure 3 AODV Routing Procedure

3. PROPOSED WORK

a. Identifying the problem

Due to its inherent strength, the VANET is vulnerable to both internal and external opponents, which poses serious technological difficulties in terms of dependability and secure paths. The attacker's driving style is a risky and expensive technique to lessen traffic on the network and raise the likelihood of having a reckless path, as opposed to road construction.

The existence of a Blackhole attacker is the cause of the violent behaviour on the network. In addition to offering safety guarantees, some nefarious or malicious vehicles undermine the system by delivering subpar services or putting the vehicles of users in perilous circumstances. Therefore, a crucial component of VANET defence is the act of detecting those vehicles that are immoral or harmful. Cruel users of automobiles may act cruelly in one way and cruelly in another. The network traffic packets are all thrown onto the network by the attacker, who also has the ability to generate fake information on the network. Due to the

packets' significant loss to the network, offensive vehicles generate overhead. Although packet redistribution reduces network delays, it is unable to eliminate traffic congestion and does not adequately manage traffic conditions due to the existence of blackholes. Proposed SDSR Detect and stop harmful vehicles to enable secure delivery of multi-hop data packets.

b. Flow chart of attacker detection

The recommended Defense Plan's flowchart shows the steps to take in order to spot the attacker's combative activity on VANET. To determine which nodes are consistently dropping packets throughout a network, detection is necessary.

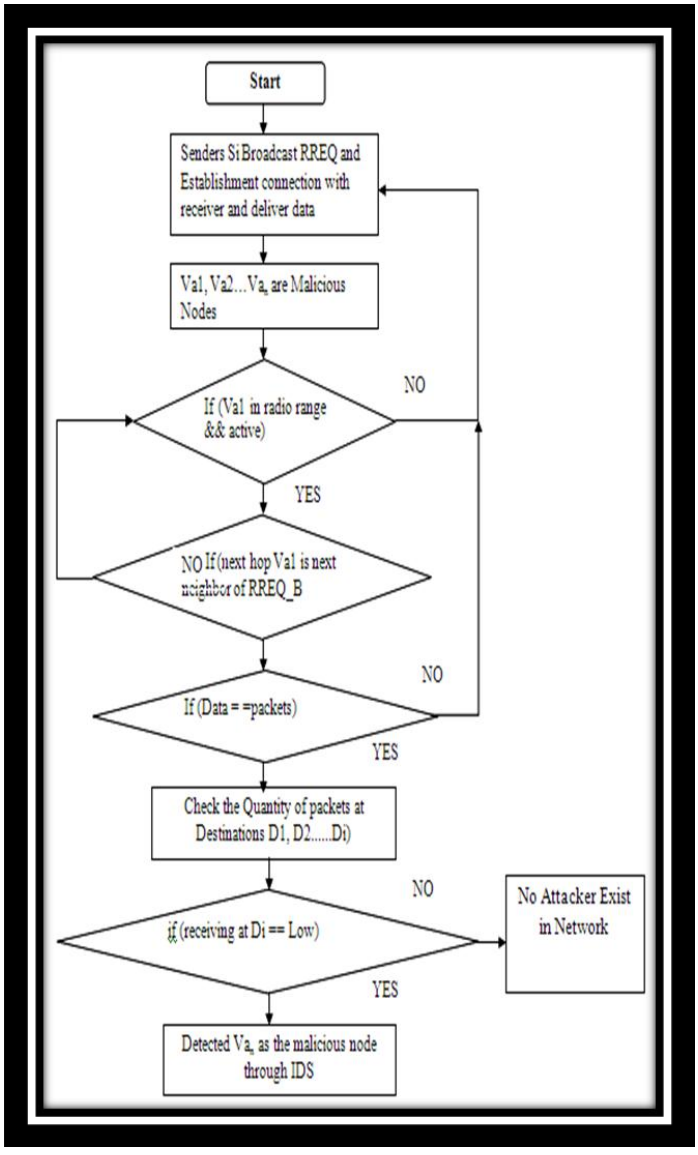

Figure 4 Flow chart of attacker detection

4. Results analysis

The prior M-AODV and Blackhole AODV are used to gauge how successful the proposed protection mechanism with the DSR route protocol is overall (BAODV). For all modules, the range of node conditions is the same. The suggested security system's overall performance serves as proof of performance.

a. Throughput Performance Analysis

Throughput, also known as network throughput, in vehicular networks refers to the rate at which a message reaches the destination vehicle across a communication channel. This data can be added over a physical or logical link or bypassed through a specific network device. The throughput is often expressed in bits per second (bit/s or bps), but it can also be expressed in statistics packets per time slot or facts packets per second. This graph shows the throughput.

Performance of the planned secure DSR, the relaxed AODV (M-AODV), and the blackhole AODV (BAODV) (DSR). If a hostile device enters the network and transmits data, the outcome may be compromised; however, if the SDSR attack strategy is used, throughput performance is once again improved. In all node density scenarios where the performance is reduced, the throughput at the time of the black hollow node in the community is minimal. The M-AODV's performance restores the network's overall performance, but the proposed system also enhances performance.

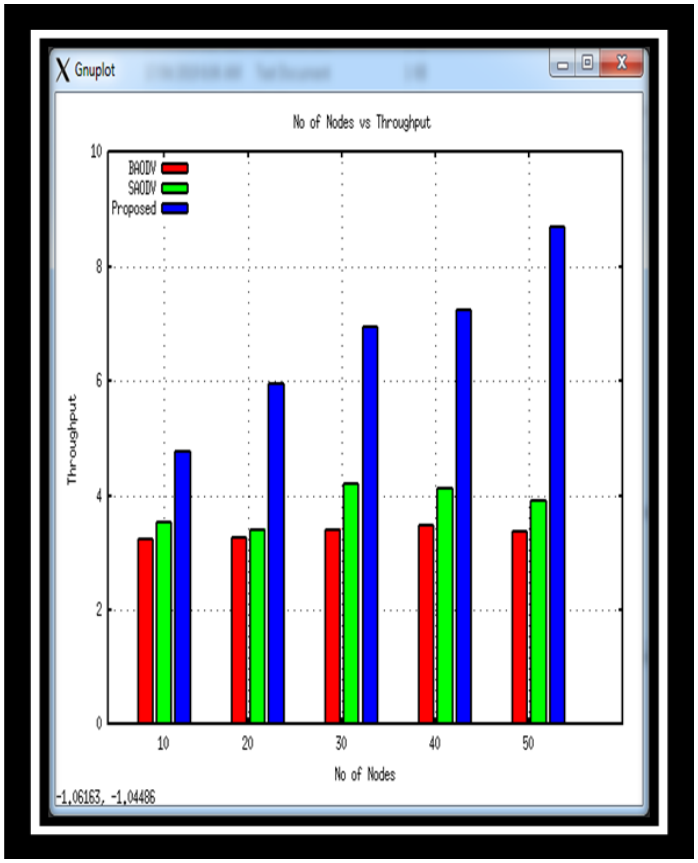

Figure 5 Packet Drop Analysis

b. Packet Drop Performance Analysis

Because of the attacker's bad behaviour, a lot of traffic status packets are dropped in the network. Vehicles regularly send and receive traffic data across the network to determine the optimum driving location on the roads, and the route protocol's presence is crucial for VANET. The potential data drop in BAODV, M-AODV, and SDSR is only evaluated on this graph.

Here, the attacker's activity on the entire network of traffic data obtained from the network lowers to only roughly 22500 packets of data. Due to the attacker's misbehaviour in releasing the data packets, vehicles is busy resubmitting the request, which is why the data is declining. However, after implementing secure SDR communication, the security standards for dependable communication were improved, and data loss was decreased in comparison to the prior security M-AODV scheme. In the case of 40 and 50 nodes, the more data losing is evident.

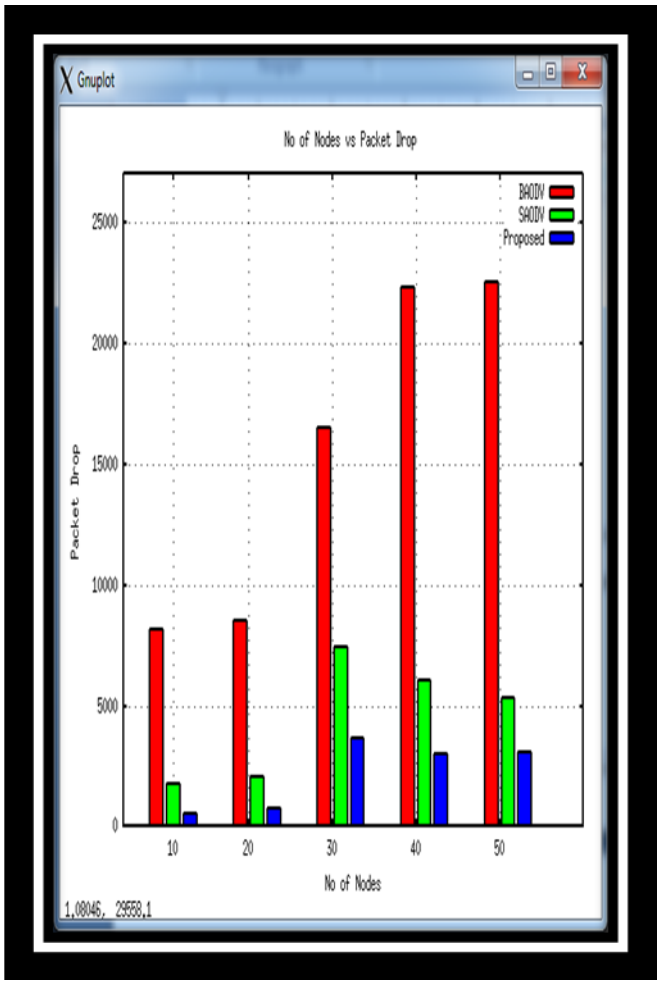

Figure 6 PDR Analysis

c. Packet Receiving Performance Analysis

Contact VANET to complete the vehicle sender request and maintain traffic on the roads. In this graph the acceptance of BAODV data is small compared to SADV and SDSR. that means that the loss of black hole data is significant and if we use the proposed SDSR for data retrieval is high, that indicates in all node congestion conditions. That indicates that receiving when dangerous nodes are not really important within the source to the point that ends the network under infection. The attacker vehicle uses data packets on the network and reduces the actual network performance but in the proposed scheme the performance increases which shows better acceptance compared to M-AODV.

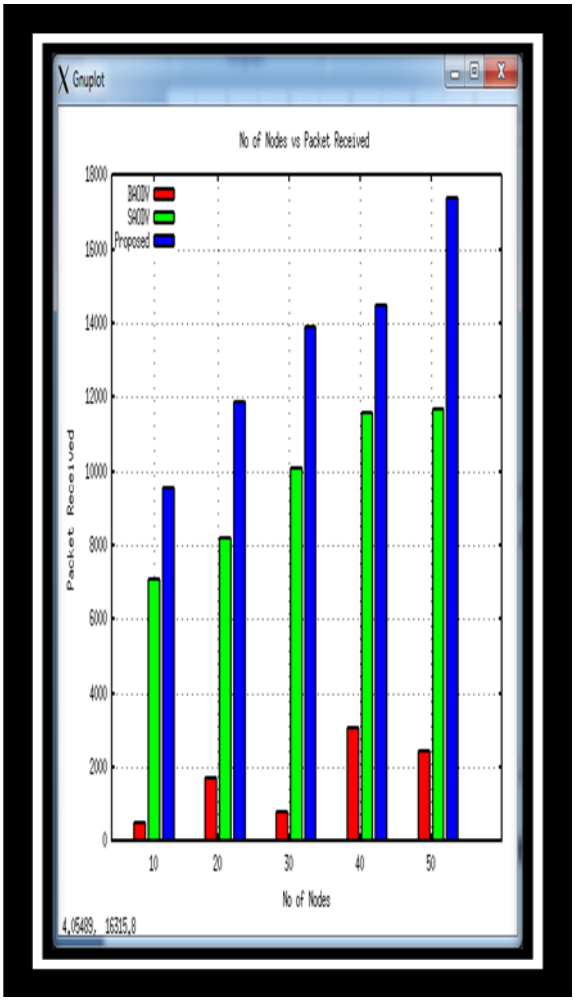

Figure 7 Packets Receiving Analysis

d. 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 sends the traffic request for recognizes the traffic status. The vehicles are drive on that path according to the traffic information of beginning vehicles. Traffic data is also detrimental if it is delivered over the network e.g. did not behave properly due to the presence of the Blackhole invader (BAODV). In this graph the performance delay is measured and it is noted that the BAODV delay performance remains high in all node

congestion conditions. The development of delays is even higher for M-AODV but the minimum for the proposed SDSR system. The proposed Blackhole attacker system protects network performance and provides the delivery of application packages in line with VANET's normal operation.

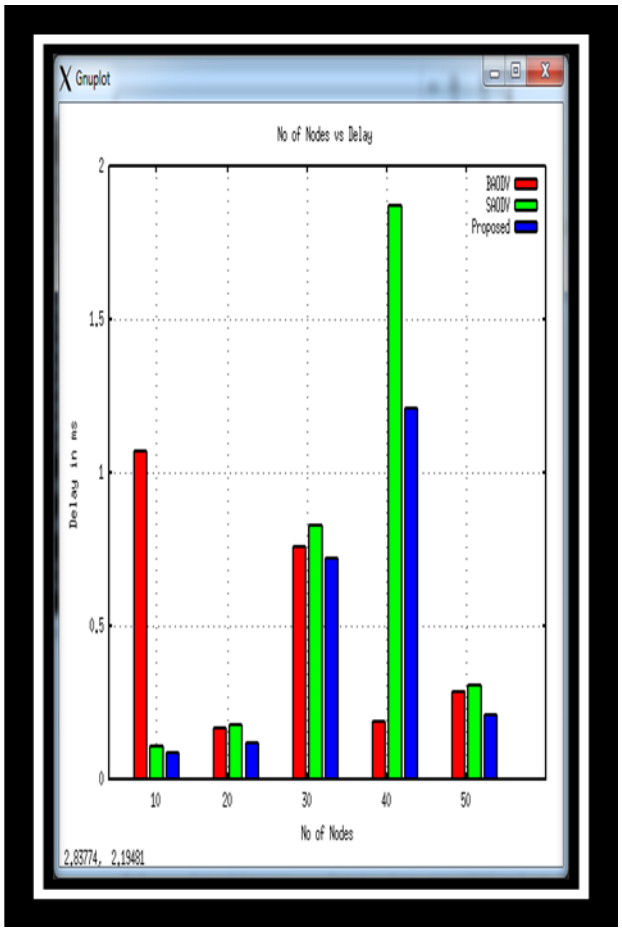

Figure 8 Delay Analysis

3. CONCLUSION & FUTURE WORK

The presence of malicious vehicles / vehicles degrades the performance of In presence of blackhole attacker packets drooping is improved and reception and transmission are greatly reduced compared to normal communication. In this study the proposed SDSR protection system identifies and prevents the network from single and multiple blackhole attacks on VANET. The proposed method is determined by the reduction of the package counting above a certain limit and then the potential attacker on the network.The number of vehicles crossing the road and terminals such as RSU units. The RSU unit monitors traffic information sent to vehicles within a certain distance to identify other traffic conditions in moving vehicles. RSU surveillance detects the presence of an attacker and subsequently blocks it. In this paper VANET's list of features such as environment, standards and network construction were discussed. At VANET to find and produce a traffic request route to form an important component used for outstanding and relevant communication. Security on VANET to improve opt-out and PDR. Improving packet handling also improves performance by reducing delays and highs .Although the attack creates a more difficult situation, it is necessary to investigate the impact of the attack on the track systems that create a secure vehicle environment. The proposed SDSR reduces packet collapse and due to the presence of the attacker the fallout closes completely and removes the invader infection from the network.

The presence of an attacker on VANET works best to detect it using a location detection system or the Global Positioning System (GPS) to identify a real dangerous vehicle or current location. The location-based system also improves additional performance during delays and highs.

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.