

Performance Analysis of Ad-Hoc Networks Under Black Hole Sybil Attack and DDoS Attack

M. Tech Scholar Vikas Swarnakar, Asst. Prof. Shivraj Singh

Department of Electronics and communication,
Technocrats Institute of Technology,
Bhopal, India
Vik.swarn@gmail.com

Abstract- The next generation communication network has been widely popular as an ad hoc network and is roughly divided into mobile nodes based on mobile ad hoc networks (MANET) and vehicle nodes based on the vehicle's ad hoc network (VANET). VANET aims to maintain traffic congestion by keeping in touch with nearby vehicles. Every car in the ad-hoc network works like a smart phone, which is a sign of high performance and building an active network. The self-organizing network, is a decentralized dynamic network, as vehicles are constantly moving, efficient and secure communication requirements are required. These networks are more vulnerable to various attacks, such as hot hole attacks, denial of service attacks. This article is a new attempt to investigate the security features of the VANET routing protocol and the applicability of the AODV protocol to detect and manage specific types of network attacks called "black hole attacks Sybil attack and DDoS attack. A new algorithm is proposed to improve the security mechanism of the AODV protocol, and a mechanism is introduced to detect attack and prevent the network from being attacked by the source node this simulation set up performed on matlab simulation.

Keywords- VANET, Sybil attack, DDoS attack, Black Hole Attack, AODV Protocol.

I. INTRODUCTION

The Vehicle Node-based Vehicle Self-Organization Network (VANET) is made up of drones that have high mobility and provide connectivity to remote areas. A drone is an airplane without a pilot on board.

The UAV can be remotely controlled (i.e. controlled by the pilot at the ground control station), or it can fly autonomously according to a predefined flight plan. Civilian uses for drones include 3D terrain modelling, package delivery (Amazon), etc.

The US Air Force also uses drones for data collection and situational understanding without the risk of flying in hostile alien environments. By integrating ad hoc wireless network technology into drones, multiple drones can communicate with each other and perform tasks and tasks as a team.

If an unmanned aircraft is destroyed by the enemy, its data can quickly evolve into new technology or air technology, surveillance of inaccessible areas or surveillance of disasters.

In this case, the Vehicle Node Self-Organizing Vehicle Network (VANET) will be displayed, which is a self-organizing network configuration composed of Unmanned Aerial Vehicles (UAVs).

II. MOTIVATION

Wireless ad hoc network (WANET) or mobile ad hoc network (MANET) is a Decentralized wireless network. The wireless mobile ad hoc network is a self-configuring dynamic network where nodes can move freely. Such a wireless network lacks the complexity of installing and managing infrastructure, enabling devices to set up and join the network "anytime, anywhere" anytime, anywhere. By definition, true MANET requires multicast routing, not just unicast or transmission.

Each device in MANET can move freely and independently in any direction, so its links to other devices change frequently. Each router must forward traffic that is not associated with its own use, so it must be a router. The challenge in set up MANET is to equip every unit to always maintain information wanted to route traffic properly.

III. METHODOLOGY

Temporary routing procedure usually work foundation on route finding or route protection. The cause node without steering information must institute a route to the destination. When the node modify, some links on activation path may be interrupted, thus starting the route maintenance process. The Adhoc On-Demand Distance Vector (AODV) routing protocol is the most widely used

topology-based routing protocol in VANET. The cause node that finds route to purpose node sends an RREQ message (RREQ) to nearby nodes and waits for an RREP message (RREP) from any node that has registered the destination path. The AODV protocol has a major drawback, i.e. basis node does not know which node is receiving the sent request packet or sending a response.

Because ad-hoc networks lack a fixed framework, there is no fixed infrastructure circuit, so AODV is vulnerable to attack. The vehicle-mounted ad hoc network is subject to a weather attack that can come from any node within the radio area of any node in network. These attacks mainly include passive eavesdropping or leakage of secret information, gray holes, black holes, wormholes and paralysis attacks. The focus of this investigate paper is to detect or prevent black hole attacks.

IV. PROPOSED SYSTEM

Long-term protocols are often sought after or maintained. A number without route information must be entered at the location. When the node changes, there is a pause in the path of activation that may be interrupted, so the maintenance process of the path begins.

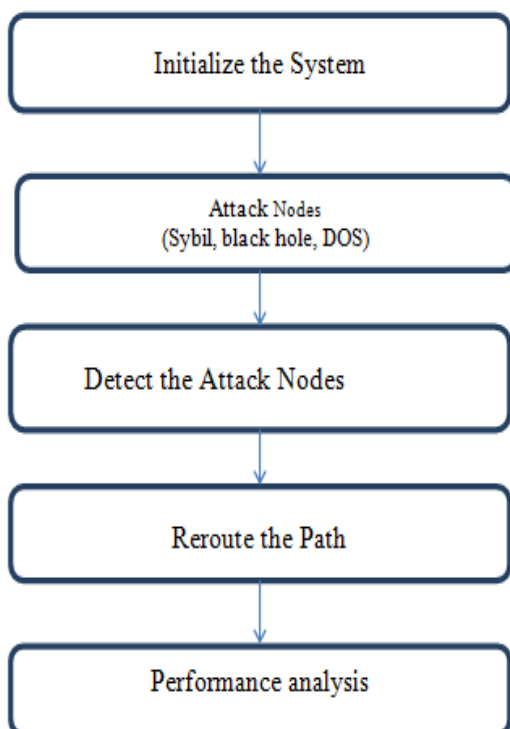


Fig 1. Proposed flow diagram.

The AODV protocol is a topology-based stored protocol that is commonly used on VANETs. The source node that finds the path to the target node sends the RREQ (RREQ) message to the neighboring node and waits for the path path (RREP) to a node that has already written the target

path. The AODV protocol has an endpoint, that is, it does not know which node receives the sent request package and sends a response. AODV is vulnerable to attack. The weather attack on ad hoc driving networks can come from a node in the network area of the network.

These attacks comprise the download and extraction of confidential information, hair holes, black holes, wormholes and denial of service. The focus of this article is on exploring and defending black hole attacks. In a "black hole" attack, the source mass sends a corner request (RREQ) to the node to find the shortest path to the location. The intermediate nodes that receive the RREQ message will send it to the nearest destination until they find a way to get to the destination.

Meanwhile, it may damage one of the intermediate nodes, and send the RREP error message to the source node. node source sends all the message packets to the malicious mouth, so it will not be sent to the recipient. Meanwhile, sources reject other RREP messages, which include the exact path to the target. The VANET black hole attack illustrates this, as well as the SYBIL and DOS attacks.

The source node A sends a RREQ message to find a way to send the data package to the of node Once the source node receives the wrong RREP, it selects the path received from the malicious node and also ignores the messages from the RREP entering the correct node. By redesigning this method, you can successfully capture other routes and packet messages within the network by forcing most of the traffic through the network.

If a bad node enters the sent RREQ message and sends a built-in RREP message, there is no natural mechanism in AODV to determine if the received RREQ is from a valid node or the malicious nodes. The focus of this research is on hitting the black hole, where the legitimate data packets will settle into the body of the victim, resulting in the loss of information. It can be dangerous to return badly due to abnormal behavior or due to damage or damage to the node. Black hole attacks are a form of denial of service in which malicious slaves falsely claim to have information to transmit information to a destination.

1. SYBIL Attack:

Devices on a peer-to-peer network are software that can access local resources. Devices advertise on peer-to-peer networks by providing identities

2. Black Hole Attack:

Zero routes or black hole routes are network routes that have nowhere to go. Matching packets are lost (ignored) rather than forwarded, which is a very limited firewall. The action of using empty routes is usually called black hole filtering. The rest of this article deals with zero routing in Internet Protocol (IP).

3. DOS Attack:

Application layer DDoS attacks are mainly targeted at specific targets, including transaction interruption and database access. It requires fewer resources than network layer attacks, but it usually accompanies them. Attacks may be disguised as legitimate traffic, but target specific application packages or features. Attacks on the application layer can interfere with services such as retrieving information or searching features on the site. [5-10]

V. SIMULATION RESULTS

In order to compare the performance of different attacks, numerous simulations were carried out. The following results compare AODV performance to non-attack environments. The current network contains a large number of malicious nodes, so its influence must be resisted. The experiments did take into account black hole attacks, Sybil attacks and DDoS attacks in the network.

The results are shown in the Fig below;

1. Network Model:

In this paper, N numbers of nodes are deployed in the network randomly under the control of and an administrator. These are well configured, energy efficient, and promising nodes in the network.

```
Num of Nodes=100;
src_node=10;
dst_node=20;
datarate=8; % packets/sec
citysize=100;
axis([0 citysize+1 0 citysize+1]);
hold on
blksiz=30;
Eini=1;% in joules
Range=20;
breadth = 0;
display_node_numbers = 1;
src_node1=src_node;
```

2. SYBIL attack:

In this simulation, 100 source nodes and 10 source nodes are acquired at a rate of 8 packets / s, 20 destination nodes are selected and the city size is 100. In this simulation against DDoS attacks, follow the following parameters for simulation

axis([0 citysize+1 0 citysize+1]).....Eq (1)

```
blksiz=30;
Eini=1 in joules
Range=20
breadth = 0;
numbers display node = 1
source node 1=
and total define attack node
sybil_node=14
```

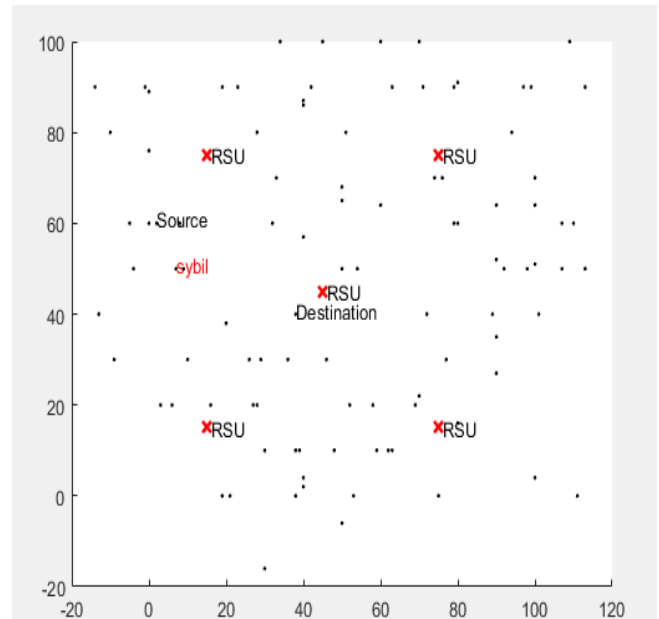


Fig 2. Highway scenario with 100 nodes with 120 km/h speed.

During this packet transaction, proposed concept checks for security parameters in the form of REQ and REP message and assure about the detection and prevention of Sybil attack by showing the fake identities of Sybil nodes. Fig 4 shows the detection & prevention of Sybil nodes.

In this simulation, 100 source nodes and 10 source nodes are acquired at a rate of 8 packets / s, 20 destination nodes are selected and the city size is 100. Fig total number of distance in each linked path for source and destination vehicle position show in Figure.2

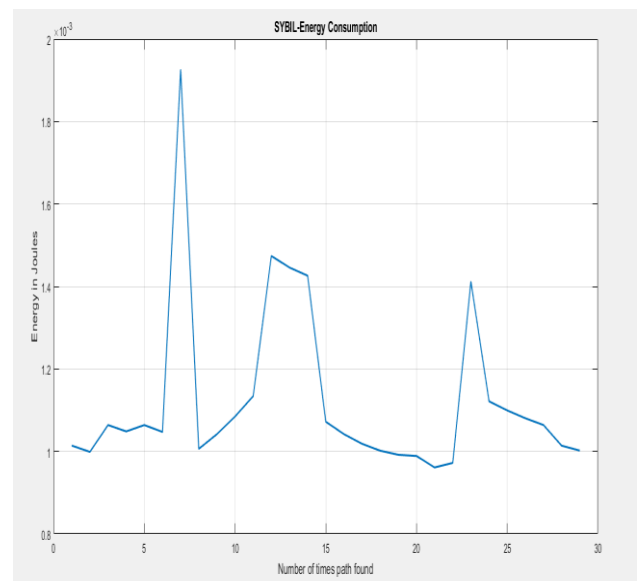


Fig.3 Energy consumption for Sybil attack.

In the Fig 3 showing the energy consumption for Sybil attack, where X axis showing the number of times path

found and Y axis showing the energy acquired by node during transmission of data.

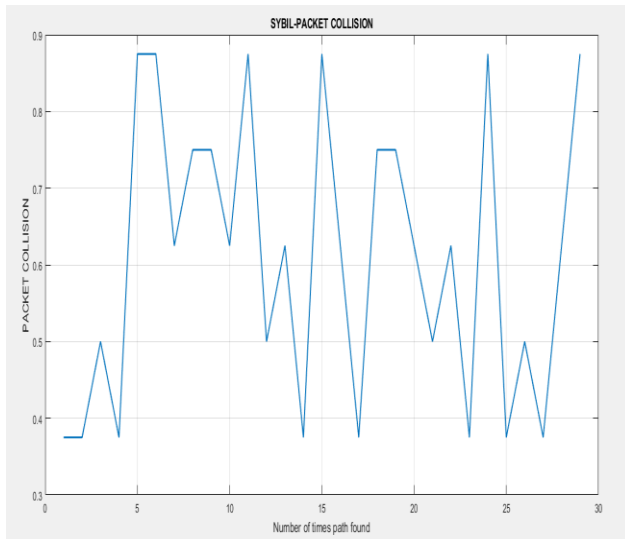


Fig 4. Packet collision for Sybil attack.

In the Fig 4 showing the energy consumption for Sybil attack, where X axis showing the number of times path found and Y axis showing the packet collision during transmission of data.

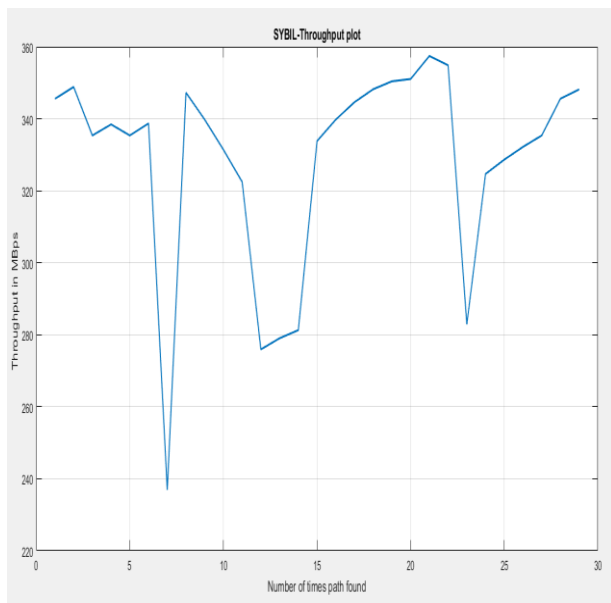


Fig 5. Throughput for Sybil attack.

In the fig 5 showing the energy consumption for Sybil attack where X axis showing the number of times path found and Y axis showing the throughput performance of the node during transmission of data.

In the Fig 6 showing the energy consumption for Sybil attack, where X axis showing the number of times path found and Y axis showing packet drop performance of the node during transmission of data.

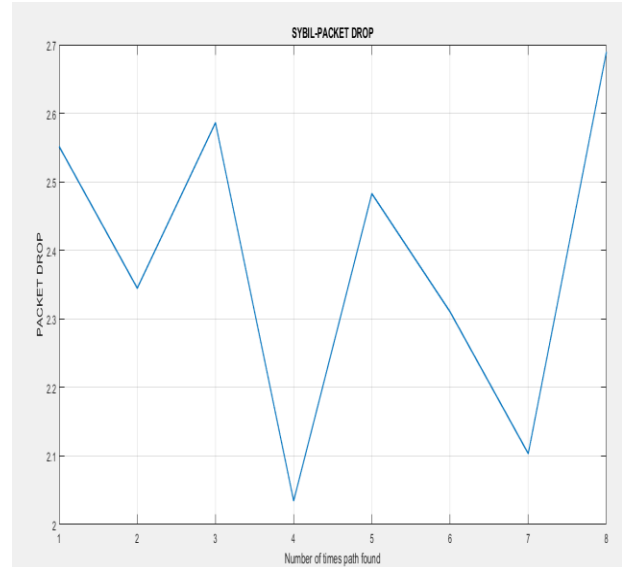


Fig 6. Packet drop for Sybil attack.

3. Black Hole Attack:

In this simulation, 100 source nodes and 10 source nodes are acquired at a rate of 8 packets / s, 20 destination nodes are selected and the city size is 100. In this simulation for DDoS attack following parameters taken for simulation.

$\text{axis}([0 \text{ citysize}+1 \ 0 \text{ citysize}+1]) \dots \dots \dots \text{Eq (2)}$

blksiz=30;
Eini=1 in joules
Range=20
breadth = 0;
numbers display node = 1
source node 1=
and total define attack node
black_node=57;

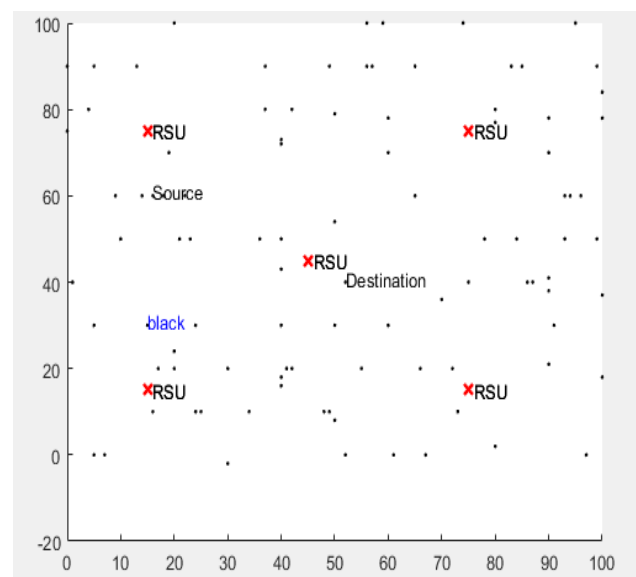


Fig 7. Highway scenario with 100 nodes with 120 km/h speed.

In this simulation Number of Nodes 100 and source node taken 10 or target node taken Devices on a peer-to-peer network are software that can access local resources. In this simulation, 100 source nodes and 10 source nodes are acquired at a rate of 8 packets / s, 20 destination nodes are selected and the city size is 100. shown in Figure.7

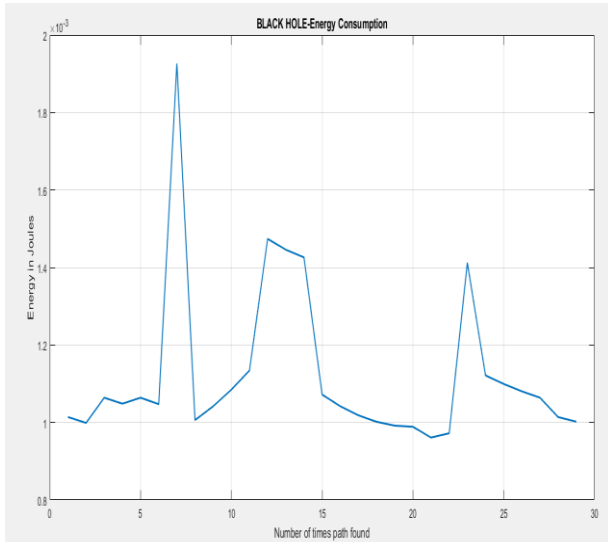


Fig 8. Energy Consumption for Black Hole Attack.

In the Fig 8 showing the energy consumption for black hole attack, where X axis showing the number of times path found and Y axis showing the energy acquired by node during transmission of data.

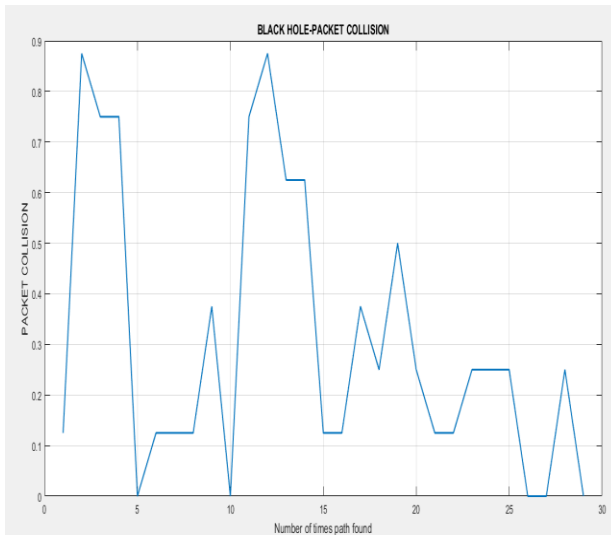


Fig 9. Packet Collisions for Black Hole.

In the Fig 9 showing the energy consumption for black hole attack, where X axis showing the number of times path found and Y axis showing the packet collision during transmission of data.

In the Fig 10 showing the energy consumption for black hole attack, where X axis showing the number of times

path found and Y axis showing the throughput performance of the node during transmission of data

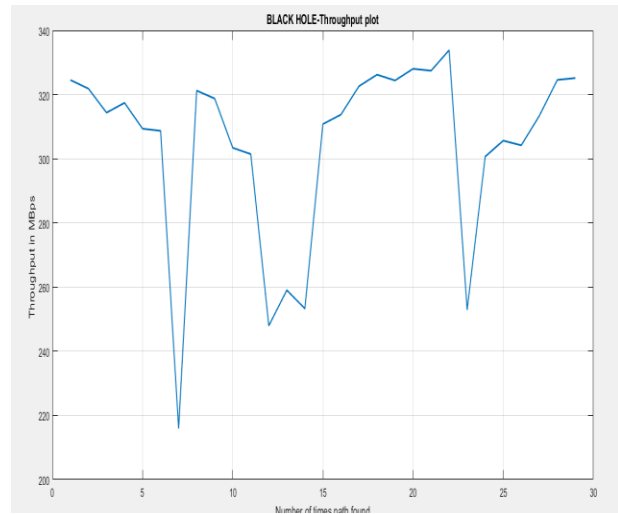


Fig 10. Throughput for Attack for Black Hole.

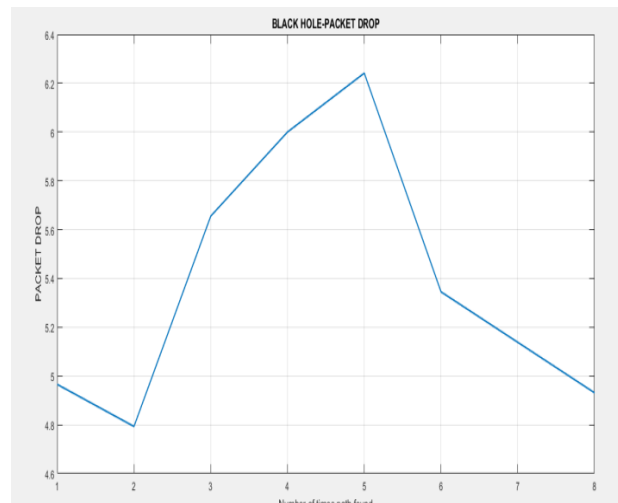


Fig 11. Packet Drop For Black Hole.

In the Fig 11 showing the energy consumption for black hole attack, where X axis showing the number of times path found and Y axis showing packet drop performance of the node during transmission of data.

4. D DOS ATTACK:

In this simulation Number of Nodes 100 and source node taken 10 and destination node taken 20 at data rate 8 packets/sec and the city size taken 100 .In this simulation for DDoS attack following parameters taken for simulation

$$\text{axis}([0 \text{ citysize}+1 \ 0 \text{ citysize}+1]) \text{)} \dots\dots\dots \text{Eq (3)}$$

blksiz=30;
Eini=1 in joules
Range=20
breadth = 0;

numers display node = 1
source node 1=
and total define attack node
dos_node=71;

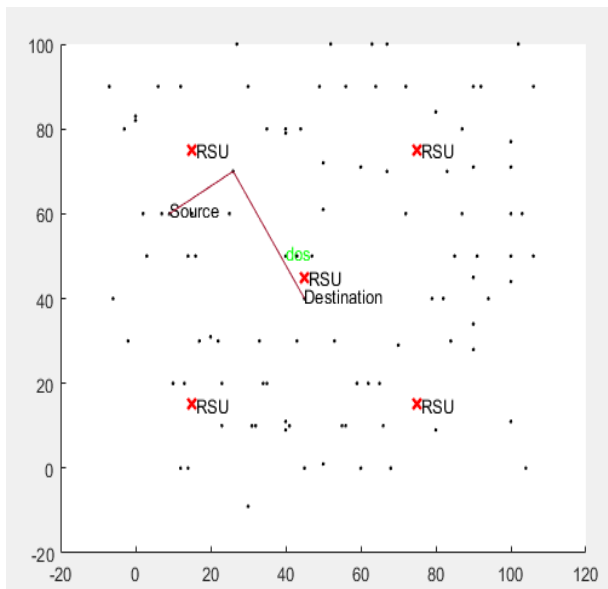


Fig 12. Highway scenario with 100 nodes with 120 km/h speed.

In this simulation Number of Nodes 100 and source node taken 10 or target node taken Devices on a peer-to-peer network are software that can access local resources. Devices advertise on peer-to-peer networks by providing identities. Show in Fig 12.

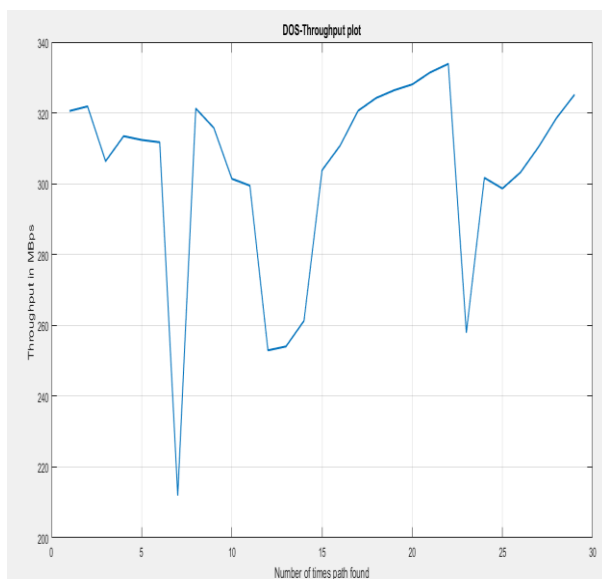


Fig 13. Throughput of Ddos Attack.

In the Fig 13 showing the energy consumption for Ddos Attack where X axis showing the number of times path found and Y axis showing the throughput performance of the node during transmission of data.

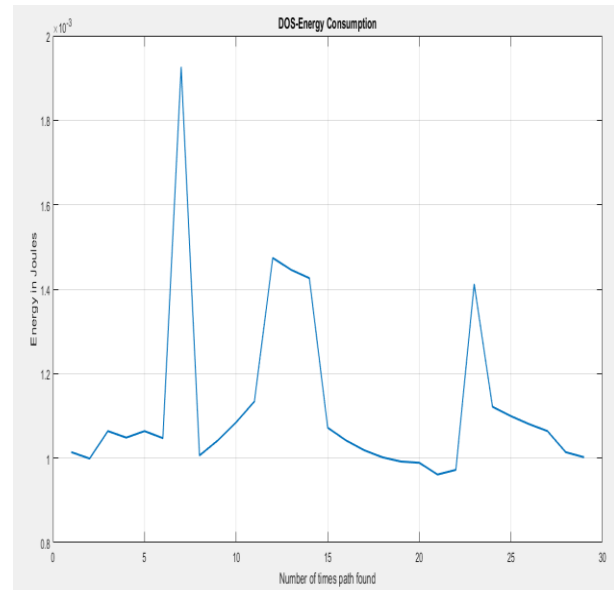


Fig 14. Energy Consumption.

In the Fig 14 showing the energy consumption for Ddos Attack, where X axis showing the number of times path found and Y axis showing the energy acquired by node during transmission of data.

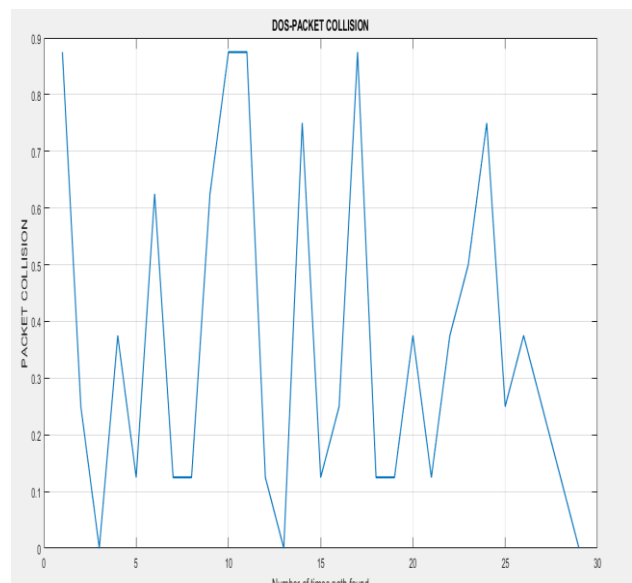


Fig 15. Packet Collision for Black Hole.

In the fig 15 showing the energy consumption for Ddos Attack, where X axis showing the number of times path found and Y axis showing the packet collision during transmission of data.

In the Fig 16 showing the energy consumption for Ddos Attack, where X axis showing the number of times path found and Y axis showing packet drop performance of the node during transmission of data However, huge numbers of necessary control packets reduce the efficiency of AODV.

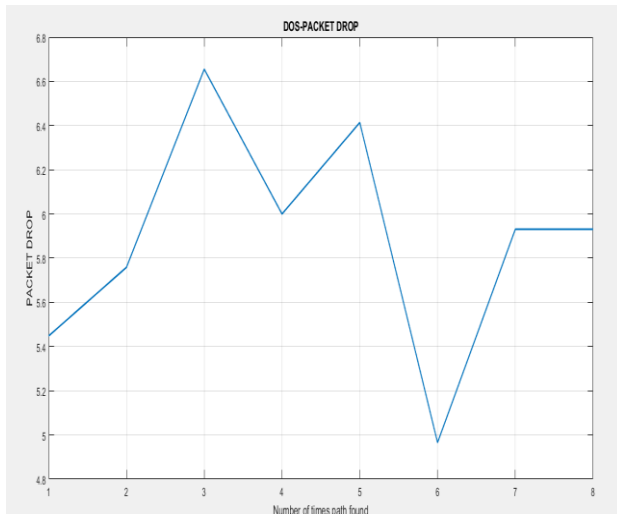


Fig 16. Packet Collision for Black Hole.

Here we found the accuracy detection for different attacks, Table 1 Comparative analysis, and table showing the accuracy for different attack.

Table 1. Comparative analysis.

	Protocol	Attack	Packet Collision	Packet Drop	Throughput Kb/S	Energy Consumption
Proposed	AODV	Sybil attack	0.89	2.4	345	1.2
		Black Hole Attack	0.88	4.9	322	1.1
Previous	AODV	Ddos	0.89	5.43	320	1.12
		Black hole	7	255	150	

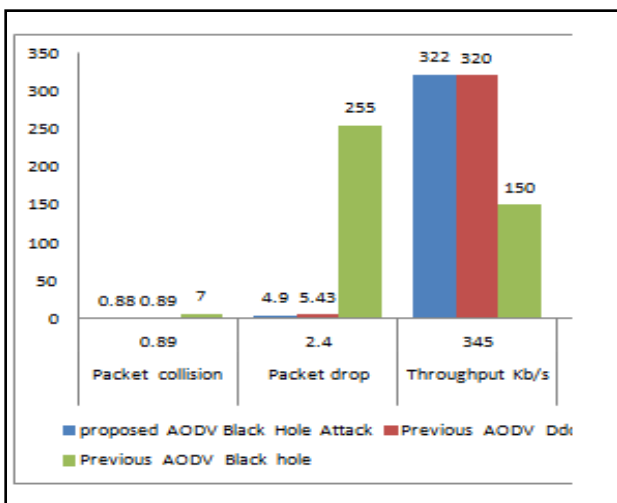


Fig 17. Comparative analysis with proposed system and existing system.

Table 2. Simulation accuracy for different attack.

Attack	Accuracy
Sybil attack	99.7
Black hole attack	99.1
Ddos attack	99.1

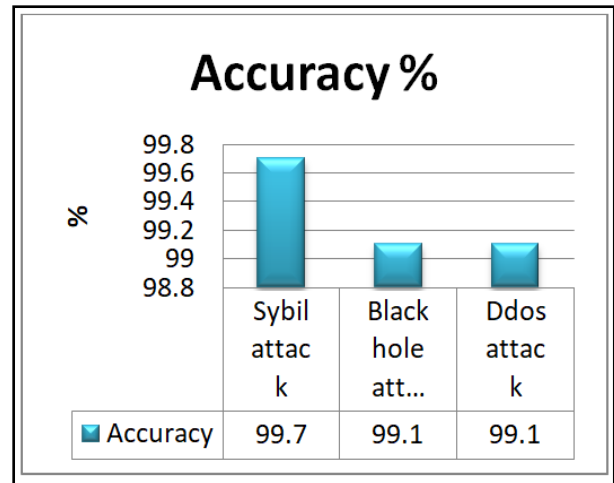


Fig 18. Accuracy for different attack.

VI. CONCLUSION

This paper discusses the performance of AODV routing protocols for highway scenarios For VANET, an algorithm is proposed to control the security features of routing protocols in VANET and the use of AODV (Ad hoc On Demand) protocol. For detection and resolution. A special type of network attacks. As it is characteristic of the VANET system structure that the topological structure changes frequently, it is very important to accurately describe, control and monitor the timing of routing updates.

References to parameters such as throughput, packet drop and packet loss. The proposed algorithm can adapt to dynamic network conditions faster using various control messages. Route protocols in VANET are more vulnerable to attack. Therefore, a new monitoring algorithm is needed. The better protection scheme is provides the complete security from attacks and the secure routing is provides the better and trustful network performance.

REFERENCES

- [1] Chlamtac, Conti M, Liu J. Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks; 2003. p. 13–64.
- [2] Zeadally Sherali et al. Vehicular ad hoc networks (vanets): status, results, and challenges. Telecommun Syst 2012; 50(4):217–41.

- [3] Paul B et al. VANET routing protocols: pros and cons. *Int J Comput Appl* 2011; 20(3):28–34. April.
- [4] Perkin Charles E. Ad hoc on demand distance vector (AODV) routing. Internet draft, draft-ietf-manetaadv-02.txt, November 1988.
- [5] Dembla Dr Deepak, Tyagi Ms Parul. Taxonomy of security attacks and issues in vehicular ad-hoc networks (VANETs). *Int J Comput Appl* 2014;91(7):22–7 [Published by Foundation of Computer Science, New York, USA].
- [6] Hong X, Xu K, Gerla M. Scalable routing protocols for mobile ad hoc networks. *Kluwer Wireless Networks* 2002;16:11.
- [7] V. Rathod and M. Mehta, “Security in wireless sensor network: a survey,” *Ganpat University Journal of Engineering & Technology*, vol. 1, pp. 35–44, 2011.
- [8] A. Modirkhazeni, N. Ithnin, and M. Abbasi, “Secure hierarchical routing protocols in wireless sensor network; security survey analysis,” *International Journal of Computer Communications and Networks*, vol. 2, pp. 6–16, 2012.
- [9] W. Niu, J. Lei, E. Tong et al., “Context-aware service ranking in wireless sensor networks,” *Journal of Network and Systems Management*, vol. 22, no. 1, pp. 50–74, 2014.
- [10] Z. A. Baig, “Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks,” *Computer Communications*, vol. 34, no. 3, pp. 468–484, 2011.