International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 2, March-April-2021, ISSN (Online): 2395-566X

Performance Analysis of Routing Protocols for Security Attacks

M. Tech. Scholar Pooja Verma, Asst. Prof. Dr. Priyanka Shivhare
Department of Electronics and Communication,
IASSCOM Fortune Institute of Technology,
Email-id – ifitbhopal@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 modeling, 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). without crew.

The aircraft is responsible for monitoring a specific area by taking an image and sending it to the ground-to-ground communication process (U2G) to send it to the base station [1]. In the context of FANET, different from traditional infrastructure and cable challenges, new challenges have emerged: (1) Position the drone in the most appropriate way to monitor the area, minimize costs and maximize network performance; (2) Reduce the negative impact of the high mobility of UAVs; (3) Due to the high mobility characteristics of nodes and topology changes, traditional routing protocols cannot efficiently handle aircraft, especially non-flying ad hoc networks.

This will damage the communication and network performance between the drones. Therefore, This fact leads to the following conclusion: nodes with low battery are no longer part of the overhead network due to their "death", so the network must automatically configure, rearrange and rearrange its topology to avoid damage that may affect the antenna Aerial Wireless communication. These metrics assess output, latency, and other objective metrics from a network perspective, but may not reflect the end user experience of the video stream or the final quality of the video received. As mentioned earlier, flight distance and manoeuvrability are factors that can seriously alter the network topology in the air.

Therefore, it is very important to establish new routing protocols to take these factors into account and to interact with changes in network topology, especially since there is currently no specific routing protocol for these temporary network scenarios that can be traced over the Internet. Traditional routing protocols, such as on-demand distance vector (AODV) and link-state optimized routing (OLSR),

© 2021 IJSRET

these protocols are neither sufficient nor effective in these situations [6]. Solve many problems: For FANETS and overhead network solutions, this article proposes a routing protocol for these solutions. The protocol was created by obscure systems for these scenarios in order to achieve the best performance among drones.

II. RELATED WORK

Because MANET has a dynamic topology and no centralized management, many studies focus on MANET.the communication problem faced by the unmanned driving system can be solved by using a self-organizing network between UAV and GBS. This is the so-called FANET, which is basically a self-organizing network between drones. Recognizing and proving the importance of a good navigation protocol for good performance on the network, a multi-UAV FANET was proposed and two types of evaluations were performed on it to use routing protocols when data packets are to be transmitted over the network. These protocols find the exact path of the various network nodes to deliver the package to the correct location.

The implementation of FANET is related to the effectiveness of the routing protocol. Effectiveness such as conversion after changing the topology, excessive bandwidth and power consumption required to perform the right path depends on a number of factors.

In fact, research on the rules of protocols has been going on for years. Several routing protocols have been proposed for this. Routing protocols can be divided into two types: active and passive.

III. 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. 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.

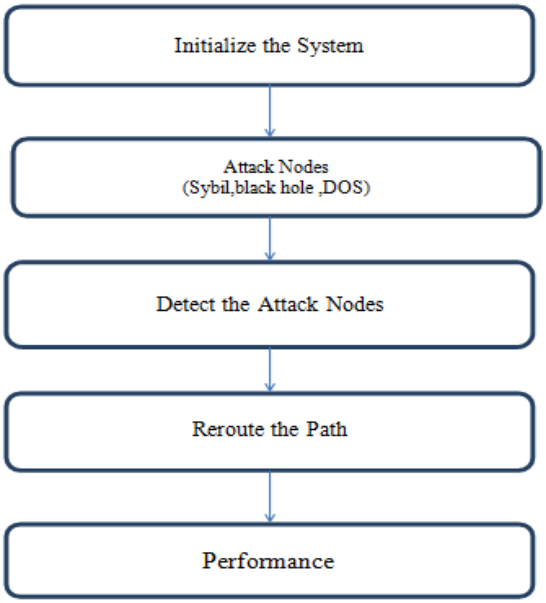

Fig 1. Proposed flow chart.

© 2021 IJSRET

1. AODV Protocol System:

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.

IV. RESULT ANALYSIS

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 not take into account black hole attacks, Sybil attacks and DDoS attacks in the network. The results are shown in the figure below;

```
Pseudo Reply Packet (PRREP) { t0 = get (current
time value)
t1 = t0 + STR_Dur
While (CURRENT_TIME <= t1) {
Store P.Dest_Seq_No and P.NODE_ID
In RREP_Tab table }
While (RREP_Tab is not empty) { if (Dest_Seq_No
>>>= Src_Seq_No) { Mali_Node=Node_Id discard
entry from M_ table } }
Select Packet q for Node_Id
having highest value of Dest_Seq_No
ReceiveReply(Packet q) }
```

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. Several identities can correspond to a device. 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

2. Black Hole Attack:

Zero routes or black hole routes are network routes that have nowhere to go. Identical packets are lost rather than ahead, which is a 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). 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. Several identities can correspond to a device. 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 simulation20 at data rate 8 packets/sec and the city size taken 100.

In this simulation for DDoS attack following parameters taken for simulation;

axis([0 citysize+1 0 citysize+1])])……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;

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. In this simulation Number of Nodes 100 and source node

© 2021 IJSRET

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;

axis([0 citysize+1 0 citysize+1])])……Eq (3)

- blksiz=30;
- Eini=1 in joules
- Range=20
- breadth = 0;
- numbers display node = 1
- source node 1=
- and total define attack node
- dos_node=71;

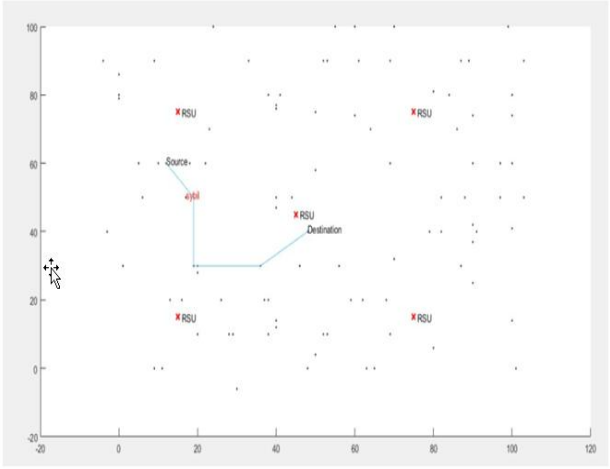

Fig 2. Highway scenario with 100 nodes with 120 km/h speed.

V. PERFORMANCE ANALYSIS

In the VANET world, there are various gateway evaluations and analytical indicators to evaluate the effectiveness and implementation of protocols in different traffic situations. This work focuses on cost reduction, package loss and accident rate collision to learn the implementation of the VANET routing protocol. the request will send to the node and the reply will from the node by the time takem to reply wil find the whether it s malicious node or not each attack has individual property if the property matches to that node the attacked path will be reroute here. The input is bits we send the bits only 105 bits taken here for request and reply.

Packet Loss: Package loss is calculated by subtracting the number of packages received at the access point from the total number of transferred.

$$\textbf{Packets losts} = \sum \textbf{Packets transmitted} - \sum \textbf{Packets received}$$

$$\textbf{Packet Loss Ratio} = \frac{(\textbf{Packets losts 100})}{\sum \textbf{Packets transmitted}}$$

Defined as the average number of bits that can be moved to the destination, which is called the hair file. The sum of the series nodes in all the networks in the network is called network access. Throughput is obtained by dividing the number of packets received by the time allotted in the simulation.

$$\textbf{Throughput} = \frac{(\textbf{received packets} * \textbf{packet size})}{\textbf{simulation time}}$$

Network throughput can also be estimated as follows:

thrgput(1,ff)=(datarate(ff)*pktsize)/time_consumed;]) …Eq (4)

In this simulation taken packet size 64 byte At different datarat like [4,6,8,10,12,14] packets/sec here 50e-9; amount of Energy consumption per bit in the transmitter or receiver circuitry. 0.0015e-12 and Amount of energy consumption for multipath fading.

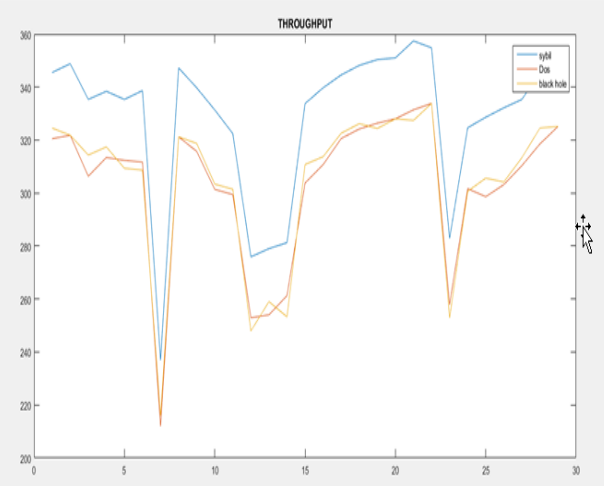

Fig 3. Throughput for Sybil, Black Hole and DoS Attack.

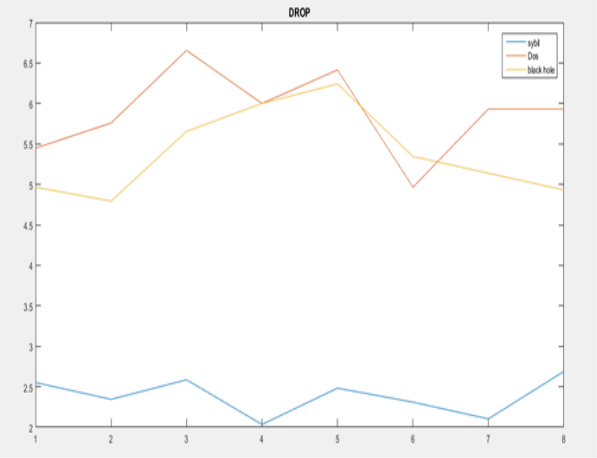

Fig 4. Throughput for Sybil, Black Hole and DoS Attack.

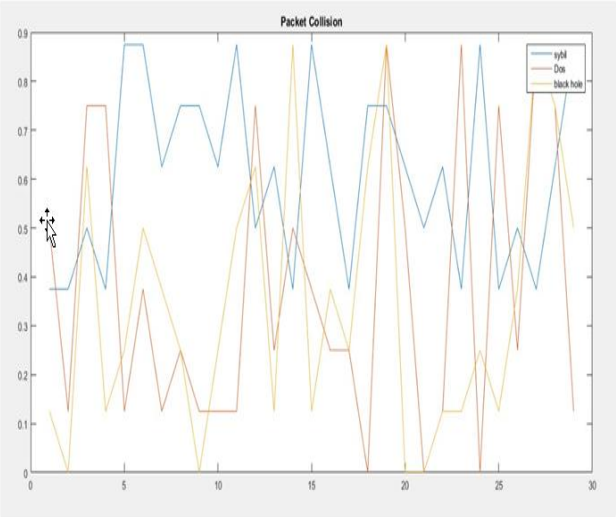

Fig 5. Packet Collision for Sybil, Black Hole and DoS Attack.

Table 1. Comparative analysis on algorithm performance.

	Protocol	Attack	Packet Collision	Packet Drop	Throughput Kb/s	Energy consumption
Proposed System	AODV	Sybil attack	0.89	2.4	345	1.2
		Black Hole, DoS	0.88	4.9	322	1.1
Previous System	AODV	Sybil, DoS	0.89	5.43	320	1.12
		Black Hole	7	255	150	

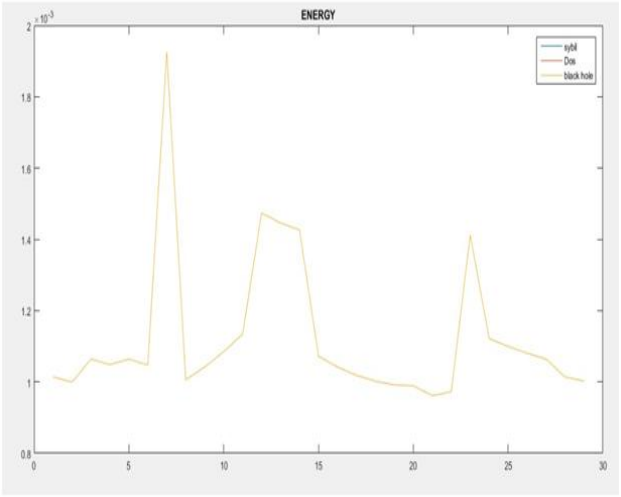

Fig 6. Energy Consumption for Sybil, Black Hole, Dos Attack.

Table 2. Comparative analysis on algorithm performance.

	Black Hole Attack	Sybil Attack	DoS Attack	Collision Rate
Shahid Latif et al. [2] introduced Authenticated Routing protocol for ad hoc Networks (ARAN). It is based on cryptographic public-key certificates	yes	yes	No	high
Lei Liu et al. [1] proposed a novel mechanism which reduces overhead but group attack was not considered	yes	yes	No	low
J. Rolimet. al. [10] resolved group attack problem with a solution to ignore the first route reply but, this method was susceptible to Black Hole Attacks	yes	yes	No	high
Alexey Vinel[11] detection of Sybil Attack in Large-Scale VANETs using Spider-Monkey Technique	no	yes	No	low
Huang L et. al [9] Improved Detection and Mitigation of DoS Attack in Vehicular ad hoc Network	no	no	Yes	high
In the proposed algorithm, overhead has been reduced and security of network for single and group attack is also been improved	yes	yes	Yes	low

© 2021 IJSRET

However, huge numbers of unnecessary control packets reduce the efficiency of AODV. Here we found the accuracy detection for different attacks table 3 showing the accuracy for different attack.

Table 3. Simulation accuracy for different attack.

Attack	Accuracy
Sybil attack	99.7
Black hole attack	99.1

VI. CONCLUSION

This article discusses the implementation of AODV protein on the road. For VANET, an algorithm offers control over the security of VANET and uses the AODV (Interim Protocol on Demand) protocol. Used for criticism and solution a kind of cyber attack. 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] Lei Liu, Chen, Tie Qiu, Mengyuan Zhang, Siyu Li, Bin Zhou," A data dissemination scheme based on clustering and probabilistic broadcasting in VANETs", in Vehicular communications, Elsevier, July 2018, doi: https://doi.org/ 10.1016/j.vehcom. 2018.05.002.

[2] Shahid Latif, Saeed Mahfooz, Bilal Jan, Naveed Ahmad, Yue Cao, Muhammad Asif, " A comparative study of scenario-driven multi-hop broadcast protocols for VANETs", in Vehicular communications, Elsevier, April 2018, doi: https://doi.org /10.1016/j.vehcom.2018.01.009.

[3] Da Zhang,Chai Kiat Yeo," Efficient replication for vehicular content distribution", in Vehicular communications, Elsevier, July 2018, doi: https://doi.org/10.1016/j.vehcom.2018.04.004.

[4] Sofiane Zaidi,Salim Bitam,Abdelhamid Mellouk," Hybrid error recovery protocol for video streaming in vehicle ad hoc networks", in Vehicular comunications, Elsevier, April 2018, doi: https://doi.org/10.1016/j.vehcom.2018.01.002.

[5] Gerlach M. and Guttler F., "Privacy in VANETs using Changing Pseudonyms - Ideal and Real", in Proceedings of the 65th Vehicular Technology 1210 Conference, VTC2007-Springer, pp.2521-2525,2017.

[6] Raya M., Aziz A. and Hubaux J.P., "Efficient secure aggregation in VANET", in Proceedings of VANET'06, California, USA 2016.

[7] Blum J. and Eskandarian A., "The threat of intelligent collisions", in IT Professional vol. 6 No.1, pp. 24-29, 2018.

[8] Hubaux J. P., Capkun S., Luo J., "The Security and privacy of smart vehicles", in Proceedings of IEEE Conference on Security & Privacy, Vol. 2, 1208 Issue 3, pp. 49-50,2019.

[9] Huang L., Sampigethaya K., Li M., Poovendran R., Matsuura K. and Sezaki K., "CARAVAN: Providing Location Privacy for VANET", in Proceedings of the Workshop on Embedded Security in Cars, 2014.

[10] J. Rolim, O. Evangelatos, C. M. Angelopoulos and. J. Buwaya, "Traversal strategies for Wireless power transfer in mobile ad-hoc networks", In Proc. ACM MSWiM'1, pp 31-40, Cancun, Mexico, Nov. 2015.

[11] Alexey Vinel, "A new routing protocol for the reconfigurable wireless networks," in Universal Personal Communications Record, 1997, Conference Record, 1997 IEEE 6th International Conference, pp. 562- 566, 2012.

[12] Mahmoud Hashem Eiza "VADD: Vehicle-assisted data delivery in vehicular ad hoc networks," IEEE Trans. Vehicular Technology, vol. 57, no. 3, pp. 1910– 1922, May 2012.

[13] Mahmoud Hashem Eiza, "Routing in vehicular ad hoc networks", A survey in IEEE Vehicular Technology Magazine, Vol.2 no.2, pp. 12–22, 2013.

[14] Manchanda P. and Bangar, P, Ü. Özgüner, G. Korkmaz and F. Özgüner, "Urban multi-hop broadcast protocol for inter-vehicle communication systems," in Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, pp. 76-85, 2014.

[15] Kamalrulnizam Abu Bakar, "Harp-hybrid ad hoc routing protocol," in Proceedings of International Symposium on Telecommunications (IST), pp. 56-67, 2014.

[16] Kashif Naseer Qureshi, Faisal Bashir and Saleem Iqbal "Cloud Computing Model for Vehicular Ad hoc Networks" in IEEE 7th International Conference on Cloud Networking (Cloudnet), IEEE Tokyo, Japan, pp.1-3, 2018.

© 2021 IJSRET