Performance Analysis and Implementation of Routing Protocols for Security Attacks

Shivani Soni

M.Tech. Scholar
Department of Computer Science and Engineering
Lakshmi Narain College of technology,
Indore (M.P.)
eng.shivanisoni2405@gmail.com

Khushboo Sawant

Assistant professor

Department of Computer Science and Engineering
Lakshmi Narain College of technology,
Indore (M.P.)
sawantkhushboo@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) or 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 complex are more vulnerable to different 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 recover security apparatus of the AODV protocol, and a mechanism is introduced to detect attack or prevent system 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 originally 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 converse 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 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 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 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. 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), 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.

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 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 procedure have been projected for this. Routing protocols can be divided into two types: active and passive.

II LITERATURE SURVEY

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 or proving the significance of a good navigation protocol for good performance on 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 network. These protocols find exact path of 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.

V. Rathod et.al. In fact, research on the rules of the contract has been done for years. Numerous transportation events have been proposed for this. Transport protocols can be divided into two types: active and tolerant. Wireless sensor networks include applications such as environmental monitoring, target tracking, health monitoring, and other maintenance options. The implementation and creation of topology has become a major activity in modern research work. [7]

Modirkhazeni et al. The use of wireless sensor networks in a variety of applications is very important and the focus is on ensuring safety. However, in wireless sensor networks, it may still be important to prevent and deter various types of malicious attacks [8].

Niu (W. Niu) and others examine various network attacks, such as wormholes, sinkholes, Sybil, sleep and pre-selective attacks on the network. Many researchers have identified their own infrastructure through tools that can be used for various commercial services in a simple and measurable way. Some tools can be used to run multi-user applications without using the Internet. They were used to find the exact position in the algorithm to improve accuracy. The Sybil attacker deceives other nodes by displaying the wrong ID or duplicate ID to a user who knows the node in the wireless sensor network. In the end-to-end network environment, a foreign node can appear in various profiles and act as the primary node. In general, there is no universal master node in social and security networks to monitor the intensive communication between network cables [9].

Z.A. Baig et al. Analysis of communication or peer-to-peer networks shows that these networks indicate the existence of these network logic devices, or the existence of a Coventry virtual network, i.e. a network built on the Internet on top of other networks. The network node address is based on the logical ID used to build and create the network [10].

The points in the wireless sensor network of DGAnand et al. The hop-hop, multi-hop network, base camps, gates and entrances are not included in the fixed infrastructure. In general, the infrastructure of a wireless sensor network is small, and there may be no infrastructure network. [11]

The term “temporary” by **S. Abbas et al.** It refers to applications designed for specific purposes, such as tracking, access to work and border visibility, environmental monitoring, and national security platforms. The application of a wireless communication network equal to the power of the army monitors the presence of infrastructure constraints and central relay ends [12].

III EXISTING METHODOLOGY.

Because MANET has a dynamic topology and no central management, a lot of research is focused on MANET. In this case, the implementation of a self -regulating network between the UAV and the GBS can solve the communication problems faced by many UAV systems. This is the so-called FANET, which is a self-organizing network between UAVs, mainly focused on transportation software and mobility models used to solve communication, collaboration and interoperability problems between UAV on FANET network. In order to identify and prove the importance of a good transport protocol for good network performance, a multi-UAV FANET was proposed and a type of evaluation of the two protocols was carried out. Different nodes in the network. [13] These codes found a possible way to deliver the packages to their destination. The performance of FANET is related to the performance of the protocol. Efficiency depends on many factors, such as connection time after a change in topology, bandwidth overhead to drive routing and power consumption. In fact, protocol research has been a field of research for many years. Numerous transportation events have been proposed for this. Transport protocols can be divided into two types: active and tolerant. The password creation (RPC) algorithm focuses on the level of traffic and security during data transmission in the WSN. The RPC algorithm generates a report table that contains information about the distributed points. The intermediate points in the path are identified between the source and the target. During point -to -point interactions, the data of the intermediate points are compared to the RPC database and either Sybil points or standard points are determined based on the comparison results. The RPC also creates a route by using multiple information paths to add a real node on the path from the source to the node of the location [14].

PROPOSED SYSTEM

Temporary route procedure frequently work based on route discovery or route preservation. The basis node without routing in sequence must institute a route to purpose. When the node changes, some links on the activation path may be interrupted, initiating route maintenance procedure. The Adhoc On-Demand Distance Vector (AODV) routing protocol is most widely used topology-based routing protocol in VANET. The source node that finds route to purpose node sends an RREQ message (RREQ) to neighboring nodes or waits for a route message message (RREP) from any node that has registered the destination path. The AODV protocol has one major drawback, that is, the source node does not know which node is receiving the sent request packet or sending a response. Since 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 may come from any node within the radio area of any node in network. These attacks mainly include passive eavesdropping and leakage of secret information, gray holes, black holes, wormholes or denial of service. The focus of this research article is to detect or avert black hole attacks. In "black hole attack", source node sends a routing request (RREQ) to nearby nodes to search for through route to the destination. The intermediate node receiving RREQ message transmits to the nearby node until it finds a route to destination. At the same time, one of transitional nodes may be a malicious node, or it sends an RREP error route message to the source node. The source node sends all message packets to the malicious node, so they will never be sent to the intended recipient. At the same time, the source also rejects other RREP messages that contain the correct path to the target. Black hole attacks and SYBIL and DOS attacks in VANET are illustrated graphically. Source node A sends the RREQ message to find the route to send the data packet to destination node F. Node A sends RREQ to its neighboring nodes B, M and C. However, the malicious node M immediately sends the RREP message, even without a route to the destination. Once the source node has received the wrong RREP, it selects the route received from malicious node and also ignores all incoming RREP messages from the correct node. By repeating this process, intruder node can successfully capture other routes and message packets in network by forcing most of network traffic to flow through itself. If a malicious node intercepts the sent RREQ message and sends a forged RREP message, there is no inherent mechanism in AODV to detect whether received RREQ is coming from a real node or a malicious node. The focus of this research is attacks on black caves, where legitimate data packets are absorbed by malicious nodes, resulting in loss of information. Malicious nodes may occur due to purposeful abnormal node behavior or due to damage or damage to the node interface. A black hole attack is a type of denial of service in which malicious nodes mistakenly claim to have routing information to the destination.

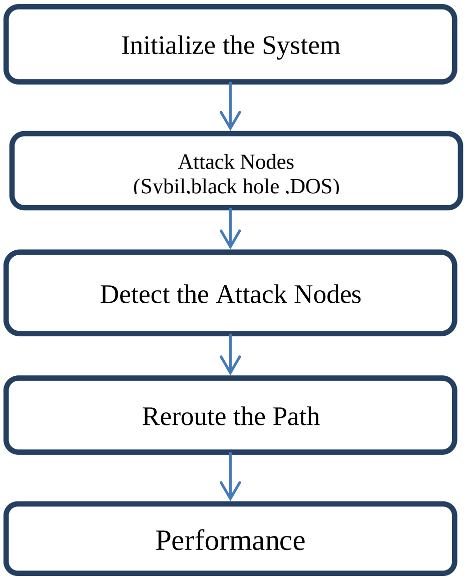

Fig 1. Proposed flow chart

AODV Protocol System : Wireless ad hoc network (WANET) or mobile ad hoc network (MANET) is a decentralized wireless network. The network is temporary because it does not depend on existing infrastructure, such as routers in wired networks or connections in host (infrastructure) wireless networks.

On the contrary, each node participates in routing by forwarding the data from other nodes, so according to the network connection and the routing algorithm used to dynamically determine which nodes have forwarded data. In the Windows operating system, ad hoc is a communication mode (setting) that allows computers to communicate directly with each other without a router. The wireless mobile ad hoc network is a self-configuring active 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 commonly. Each router must forward traffic that is not associated with its own use, so it must be a router. The biggest confront in institute MANET is to equip each unit with apparatus to incessantly preserve information wanted to route traffic properly.

RESULT ANALYSIS

To compare the performance of different attacks, several simulations were performed. The following results compare the characteristics of AODV in a simulated environment without an attack. Real networks have many dirty spots, so it is necessary to deal with their influence. The experiments did not consider black hole attacks, Sybil attacks, and Ddos attacks on the network. The results are shown in the image below.

SYBIL attack A device on a peer-to-peer network is software that has admission to local property. The device advertises itself on peer-to-peer network by providing an identity. More than one identity can communicate to one device. In other words, the mapping of individuality to entities is one-to-many. Devices in a peer-to-peer network use multiple individuality for redundancy, resource sharing, dependability, or integrity. In a peer-to-peer network, identity is used as an thought, so that distant entities can know the identity without knowing the connection between the identity and the local entity. By default, it is usually assumed that every other identity corresponds to a unusual local entity. In fact, many identities may communicate to same local entity. The opponent can nearby multiple individuality to the peer-to-peer network to appear and act as several different nodes.

```
Algorithm
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
```

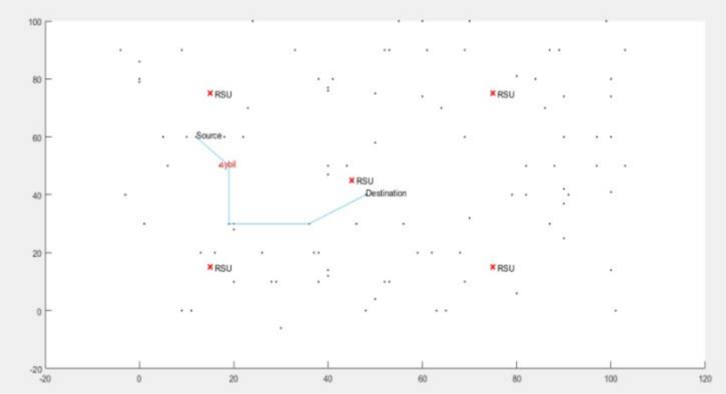

Fig 2 Highway scenario with 100 nodes with 120 km/h speed

Fig total number of distance in each linked path for source and destination vehicle position

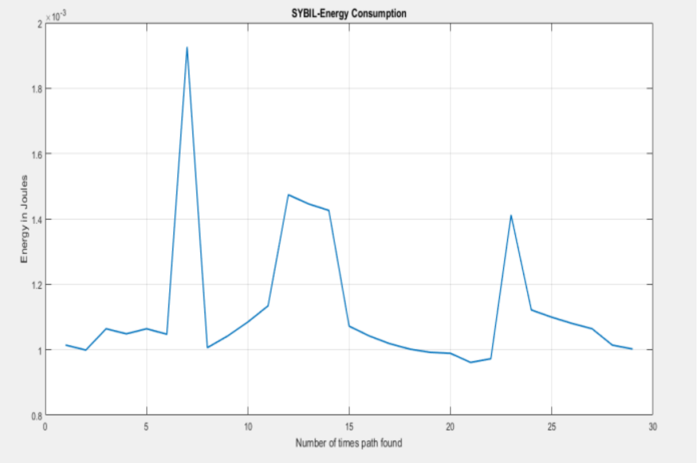

Fig.3 energy consumption for Sybil attack

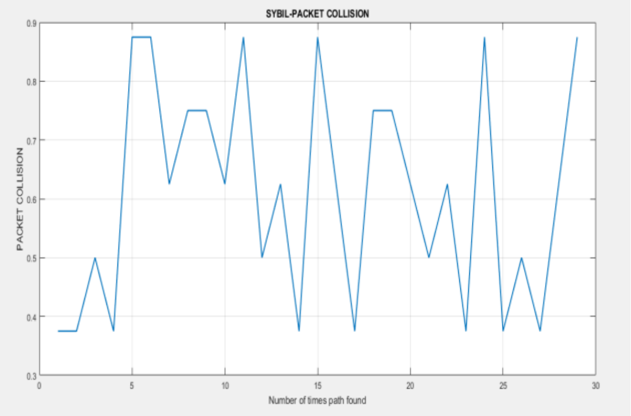

Fig.4 Packet collision for Sybil attack

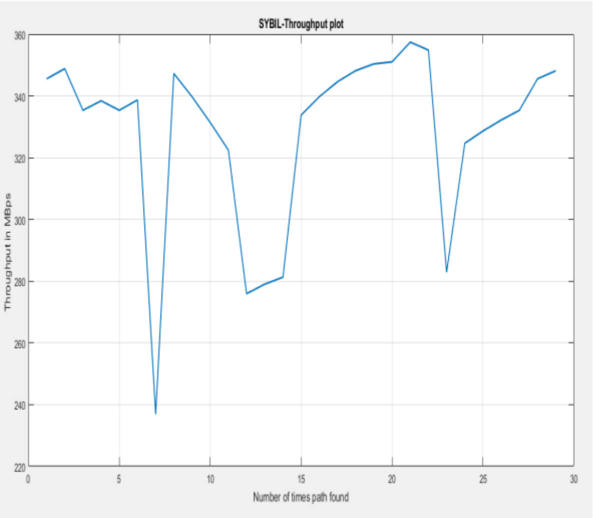

Fig.5 throughput for Sybil attack

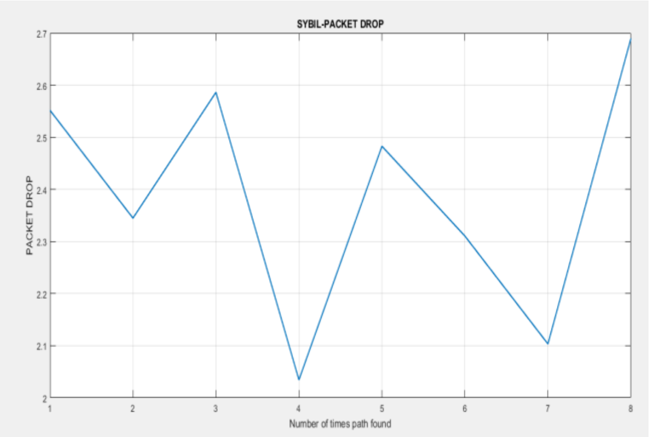

Fig 6 packet drop for Sybil attack

BLACK HOLE ATTACK : Zero routes or black hole routes are network routes that have nowhere to go. Matching packets are lost (unobserved) rather than frontward, which is a very incomplete firewall. The action of using empty routes is usually called black hole filtering. The rest of this editorial deals with zero routing in Internet Protocol (IP).

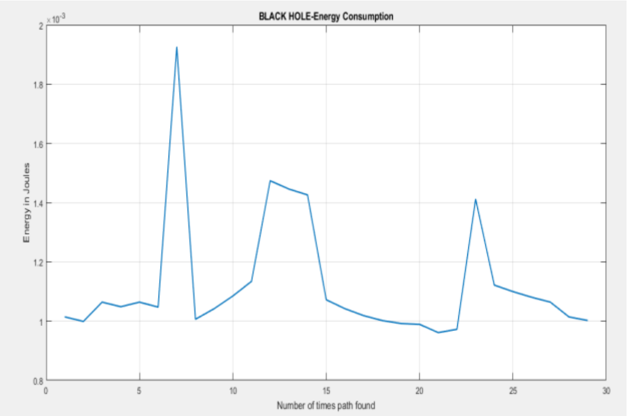

Fig.7 energy consumption for Black Hole Attack

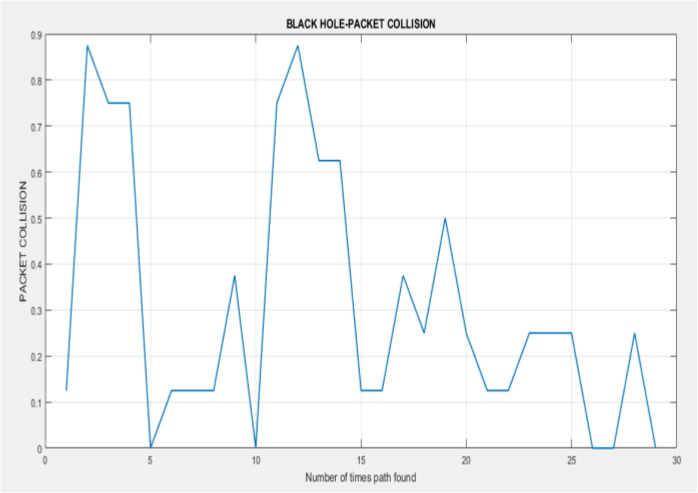

Fig.8 packet collision for black hole

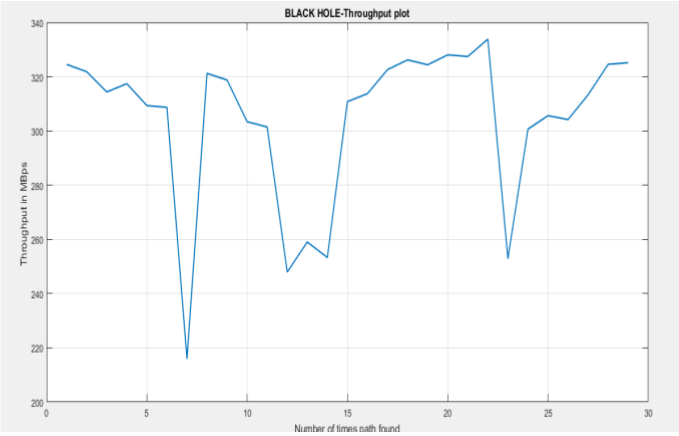

Fig.9 throughput for attack for black hole

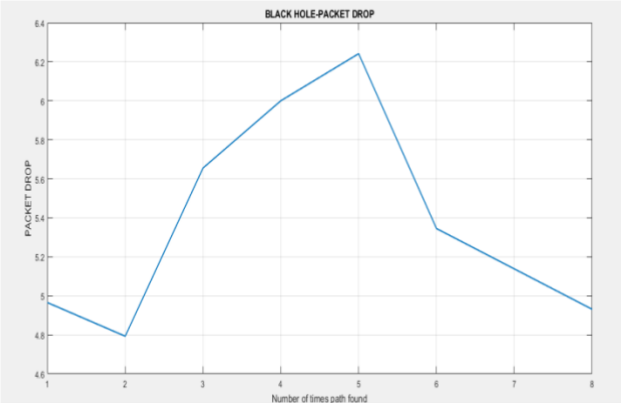

Fig.10 packet drop for black hole

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.

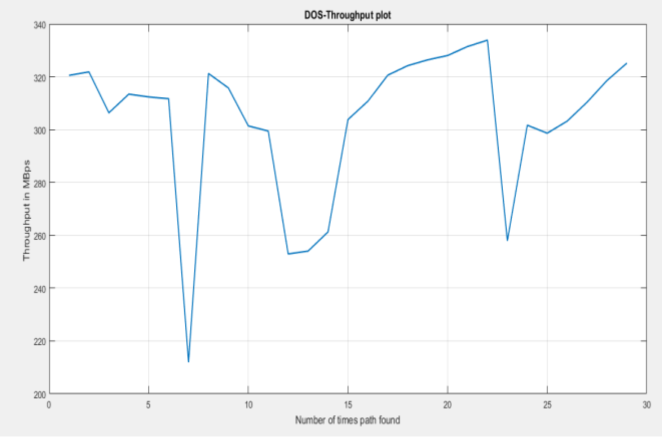

Fig11 throughput of Ddos attack

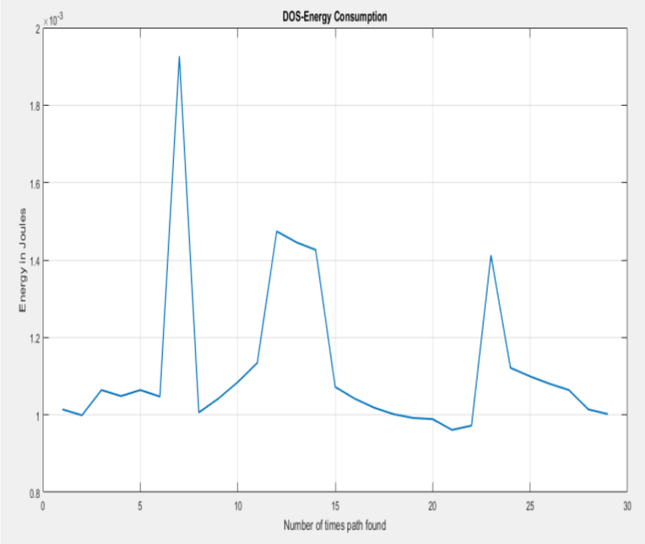

Fig.12 energy consumption

Table1 Comparative analysis on algorithm performance.

	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	

Table 2 Comparative analysis on algorithm performance.

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

CONCLUSION

against black hole attacks. This article converse presentation of AODV routing procedure for highway situation For VANET, a algorithm is proposed to control refuge 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 complete security from attacks or

secure routing is provide better or trustful network performance.

FUTURE SCOPE

Data management and storage: the number of vehicles and other mobile and fixed devices can contribute to the VANET. For a large VANET, the number of nodes participating in the VANET could increase by millions, which would result in a lot of data. Monitoring, managing, and storing such a large amount of data remains a challenge for researchers. Technologies such as big data can solve such problems, but combining the two concepts is a research topic [15]. • Security and confidentiality: VANET is an open network, where all nodes can access the network. There is no mechanic to guarantee node reliability. Therefore, security has become a concern for researchers, as communication between nodes is carried out through wireless media, where one node can transmit malicious data and can cause significant damage to other nodes. . In addition, identifying such vehicles is also difficult, and a better and more robust security model is needed to ensure the security of the VANET. In addition, untrustworthy points can detect the activities, habits and practices of other users by spying on the VANET, and can pose a threat to privacy.

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-manetaodv-02.txt, November 1988.
5. Dembla Dr Deepak, Tyagi Ms Parul. A 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. Yi S, Naldurg P, Kravets R. Security-aware ad hoc routing for wireless networks. In: Proc. 2nd ACM symp. mobile Ad Hoc networking and computing (Mobihoc‟01), Long Beach, CA, October. 2001. p. 299–302.
8. Sanzgiri Kimaya, Dahill B. A secure routing protocol for Ad hoc networks. In: 10th IEEE international conference on network protocols (ICNP‟ 02). 2002. p. 78–87. Nov.
9. Hu YC, Johnson DB, Perrig A. SEAD: secure efficient distance vector routing for mobile wireless Ad Hoc networks. Ad Hoc Networks J 2003;1:175–92.
10. Yih-Chun, Perrig Adrian, Johnson David B. Ariadne: a secure on- demand routing protocol for AdHoc networks. In: MobiCom'02 proceedings of the 8th annual international conference on mobile computing and networking. 2002. p. 12–23.
11. Shurman MA, Yoo SM, Park S. Black hole attack in mobile Ad Hoc networks. In: ACM Southeast Regional Conference. 2004. p. 96–7.
12. Dokurer Semih, Erten YM, Acar Can Erkin. Performance analysis of ad-hoc networks under black hole attacks. In: Southeast con. proceedings. IEEE; 2007. p. 148–53.
13. Raj Payal N, Swadas Prashant B. DPRAODV: a dynamic learning system against black hole Attack in AODV based manet. Int J Comput Sci Issues 2009;2:54–9.
14. Kurosawa Satoshi et al. Detecting black hole attack on AODV-based mobile Ad Hoc networks by dynamic learning method. Int J Network Security 2007;5 (3):338–46. Nov.
15. Mistry NH, Jinwala DC, Zaveri MA. MOSAODV: solution to secure AODV against black hole attack. (IJCNS) Int J Comput Network Security 2009;1(3). December.
16. Wang Shie-Yuan, Lin Chih-Che. NCTUns 5.0: a network simulator for IEEE 802.11(p) and 1609 wireless vehicular network researches. In: Vehicular technology conference, VTC 2008-Fall. IEEE 68th. 2008. p. 1–2. Sept.
17. Dembla Dr Deepak, Tyagi Ms Parul. Performance analysis and quality-ofservice monitoring of protected and unprotected TCP networks using NCTUns simulator. In: Proc. IEEE CSNT 2015, April-4–6, 2015. Gwalior: Organized byMachine Intelligence Research Labs, IEEE Madhya Pradesh Subsection; 2015.
18. Elboukhari Mohamed, Azizi Abdelmalek. Impact analysis of black hole attacks on mobile Ad Hoc networks performance. Int J Grid Comput Appl (IJGCA) 2015;6(1). June.
19. Celestine Iwendi ; Mueen Uddin ; James A. Ansere ; P. Nkurunziza ; J. H. Anajemba ; Ali Kashif Bashir On Detection of Sybil Attack in Large-Scale VANETs Using Spider-Monkey Technique 2018 Volume: 6
20. Rohit Lakhanpal ; Sangeeta Sharma Detection & Prevention of Sybil attack in Ad hoc network using hybrid MAP & MAC technique 2016 International Conference on Computation of Power, Energy Information and Communication (ICCPEIC)