IDSAODV: A Secured and Efficient Method for Detecting Blackhole Attack in MANET

Raj kumar Sharma
Dept. of CSE & IT
MITS, Gwalior
Gwalior, India
rajsharmamorena@gmail.com

Asst. prof. Jaimala Jha
Dept. of CSE & IT
MITS, Gwalior
Gwalior, India
jaimala.jha@mitsgwalior.in

***Abstract*—Autonomous mobile nodes constitute a temporary network without fixed infrastructures, as ad hoc networks. Each mobile node is independent and therefore both act like host and router. Because of this behavior, security is the major difficult task in such networks, in which every node can able to add or left the network without permission. Black Hole Attack is now one of MANET's big security concerns. It happens when the black hole connects to the network. This node runs like it has the path to the target and then takes all of the packets and therefore does not transmit to the intended location, but keeps dropping all the packets during the phase of route discovery. In this research, we simulated the attack by proposed routing method called IDSAODV using NS2, keeping in mind the network & attacker mobility with the attacker location & eventually the number of attackers. Despite the identification of the black hole attack to restart the delivery of data, the test results demonstrated that there is a circumvention of the black hole node but a reopening of the path to the real destination. Finally, we have achieved overall high performance in terms of throughput, packet rate & end-to-ends delay for all scenarios.**

Keywords*—Mobile Adhoc Network, AODV, Blackhole Attack, Blackhole Attack Detection, ISDAODV.

I. Introduction

Ad-hoc wireless networks are a self-managed community of nodes without any infrastructures. MANETS are random & interactive, which means that any nodes could be added or left at a certain point. As just a result, these have been used extensively in military & rescue regions wherever coordination is needed between soldiers in war regions and also in regions where only a new local network can collapse because of such a disaster. Ad hoc networks are local networks that are set up without even a wired network [1].

One of the most common safety risks in MANETs is the black hole attack. The attackers use the hole to do their misbehavior because it is important and unavoidable to find the path. Most scholars have pointed out various methods of detection to suggest various forms of detection methods [2].

Blackhole nodes in MANET are the mobile node which presents more updated information by presenting higher sequence number value (higher sequence number means more updated information and less sequence number means less update information in the routing table). Blackhole node changes his sequence number means present flack sequence number so node maintains path through black hole node because it contains a higher sequence number. Neighbor nodes pass data packet through black hole and black hole node drop that data packet. In a mobile ad hoc network (MANET) single or multiple black hole nodes may be present they work singly or cooperatively. So the detection of black hole nodes in MANET is an important issue [3].

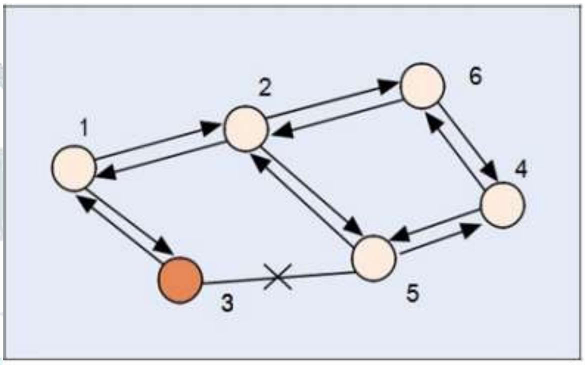

Fig. 1. The black hole problem

The adhoc on-demand distance vector (AODV) routing protocol is the routing protocol in MANETs. It is an on-demanding routing protocol initiated by the source. AODV is, therefore, susceptible to the popular blackhole attack. A suspecting node catches but does not pass packets into the network throughout blackhole attack and advertised itself as the shortest route to the node whose packets it wishes to receive. The harm will be extremely severe when more than one attacker node is working together as a group. The attack is regarded as a co-operative black-hole [4].

II. Blackhole Attack in AODV

MANET is vulnerable to a lot of security threats because of security problems. One of the other attacks is the Black Hole Attack. It is a basic and successful service denial attack where a malicious node is instructed to have the shortest path to or the node of the packets it wishes to intercept via its routing algorithm. It pretended must have a certain destination with enough fresh paths. It is presumed that the sender node is valid and also the data packets are sent to a node that would not exist, leading the data packets to be dropped. When the communication is initiated by a source node, an RREQ request for route discovery is transmitted. Once this RREQ packet is received by a malicious node, the malicious node immediately responds to the node as just a target or the shortest path for the target node with a false RREP reply. When the node does not have to search its routing table before such a routing request has been replied to, it is often the first to react in comparison to other nodes. When this RREP is received by the requesting node, it suspends its routing discovery so avoids all the other RREP messages from many other nodes. The data packets are then sent off to the 'hole,' from which the malicious node is not dispatched or absorbed. Many nodes also concurrently send RREQs; the attacker node is capable of responding to everyone's requested nodes instantly with fake RREP and therefore accessing all routes quickly. This bluffs source nodes with malicious nodes, causing a large loss of data in a lot of network traffic. Black Hole nodes may also act as a network community. The Collaborative Black Hole or Black Hole Attack [5] with many malicious nodes is a form of attack.

The black hole attack is primarily aimed at draping packets as well as interrupting communication between nodes, with all traffic in the network diverted to one particular node that does not exist. The black hole node deals in 2 examples. The 1st one is the one where the node takes advantage of the maximum insecurity of an Adhoc network, like announcing the legitimate destination node path for the node. AODV protocol's Black Hole Attack could be categorized into 2 categories: RREP black hole & RREQ black hole attack [6].

III. Literature Survey

S. Shrestha et al. (2020) recommended an algorithm that is based on a strategy for the change of the given sequence no. present in control packets in specific the AODV routing protocol Route Reply Packets, intending to find blackhole nodes and therefore minimize the loss of data by eliminating the path of these nodes at Blackhole. The outcomes of these simulations indicate that the performance of recommended methods in the AODV legacy IDS [7].

A. M. El-Semary and H. Diab (2019) Suggested a stable BP-AODV MANET routing scheme, following its current Aodv Routing protocol, to resolve data breaches of the SAODV Protocol. The BP-AODV can also defend itself with a blackhole co-operative attack that was initiated mostly during the setup phase and protects from blackhole attack mostly during the forwarding process. By enhancing the usability of the AODV protocol by using chaotic map functions, BP-AODV was created. The testing findings ensure that now the BP-AODV routing protocol is securer than that of the SAODV routing protocol and therefore could combat blackhole connection throughout routing processes effectively using susceptible nodes or co-operative malicious nodes. The findings also suggest that perhaps the BP-AODV could be very careful against blackhole attacks mostly during the transmission process [8].

Qussai M. Yaseena and Monther Aldwairi (2018) Discussed this issue and recommended the development of a global credibility scheme that would help the AODV protocol choose the best path to the destination where more than one route could be found. It facilitates the usage of the watchdogs on AODV by gathering findings and distributing them via a low overhead approach to all nodes in the network. Besides, the proposed protocol tackles the problem of detection if the black hole moves constantly. [9].

G. Bendale and S. Shrivastava (2016) Problems escalate as nodes are mobile and bad routing methods allow users to alter or convert data transmission information when network communications information is transmitted during intermediate routers wherever a node can exit or enter a network whenever the black hole attack is constant intimidation in ad hoc networks that could effectively be used for the creation of vulnerabilities. Implementation of the proposed principle is based on the alteration of the AODMDV routing protocol in NS-2 [10].

P. R. Dumne and A. Manjaramkar (2016) Suggested an approach for addressing the problem using the DSR Mechanism-Cooperative Bait Detection System (CBDS) malicious node detection scheme using hybrid protection architectures. CBDS technique aids with a reversed tracing technique to locate the malignant node. In NS-2.35 are introduced the simple and recommended CBDS schemes. Results are analyzed based on throughput, PDR [11].

Vimal Kumar and Rakesh Kumar (2015) Researchers explicitly address security issues in the MANETs to offered security against such an intruder & several strategies for secured network protocols are proposed. Their research framework provides an effective approach for detecting a black hole attack in the MANET with lower transmission costs, which is highly susceptible because of its mobility & mutual dynamic nature as opposed to infrastructure-based networks. As an opponent, the network will efficiently implement a black hole attack. It has been shown that the research suggested is safer than that of the existing strategies. They even measured its performance to the standard protocols for AODV routing. The test outcomes indicate that the approach suggested is greater than traditional AODV [12].

H. P. Singh and R. Singh (2014) this paper aims to avoid the black hole nodes and also the study of the parameters of the preceding used during the suggested technique including throughput, E2E delay, and also the PDR, but also of the BS & relative distance (RD) methods of clock synchronization [13].

P. N. Patil and A. T. Bhole (2013) established a novel solution focused on path cache to blackhole prevention in the DSR protocol. When the blackhole node is identified in the MANET, the blackhole node identity has been transferred to the DSR trace feature mostly during route formation. This feature allows routes to be connected to the cache, and that each route is determined before putting in a trace cache by scanning such routes for blackhole node id involvement. This method simply takes advantage of the usual cache time. Here, they presented the DSR routing algorithm for MANETs for blackhole prevention depending on a cache [14].

D. Kshirsagar and A. Patil (2013) developed a scheme of measuring accused nodes by their neighboring node for detecting & preventing Blackhole attacks in real-time. To simulating detection & prevention techniques, the AODV routing protocol has been changed. In real-time, the node meets the RREQ measured by source. RREP sender node's neighboring node is accused node detection [15].

P. K. Singh and G. Sharma (2012) Suggested a black hole attack solution, AODV protocol for MANETs, is one of the most popular routing algorithms. The suggested technique has used promiscuous mode in which susceptible nodes have detected (black hole) and spreads susceptible nodes information to every other node within the network. The results of the simulation demonstrated that the effectiveness of the suggested procedure because, in the presence of a black hole, the network throughput doesn't quite worsen [16].

IV. Proposed Methodology

The Secured AODV Routing Protocol is presented in this section to improve the security of the AODV Protocol. In the proposed ISDAODV scheme an AODV protocol for detecting the black hole attack for MANET has been implemented.

A. Problem Statement

The routing functions are severely threatened by Black Hole attacks by attacking the reactive protocols that lead to devastating fall in data packets. The attackers modify the behavior pattern by incorporating itself as that of the node to the destination node in this type of attack (black hole attack). Attackers can make the network suspicious. Some of the many protocols are that AODV routing also makes these attacks simple. In this type of attack, a node will announce the quickest path for the RREQ (route request) & divert the data path to the data being transmitted easily.

B. Proposed Methodology

In the proposed scheme, we have used an alternative path and promiscuous mode solution for detecting the black hole attack. If the density of the network (no. of the node) less, when we use the alternative path to ignore the black hole attack, we have dropped the first path and chose the second shortest path to send the packet. It avoids the possibility of a black hole attack.

here we have used a promiscuous node in case of several numbers of nodes if the A node is inside the B node, the communication has done from and to B, it can also be overheard even though the communication doesn't include A explicitly. If the sender node has target node info then the sender node must locate the path to the target node in the proposed IDSAODV approach. The sender node spreads the RREQ packet to scan the path to the target node & initializes the timer in the route request to check RREP time-out. For an AODV routing, the RREP to the sender node is permitted for all intermediator nodes with a correct RREP to their destinations or target nodes. In this algorithm, if the route is from the initial target then the route has presumed to be secure and ends the data using this route. Instead of that, the RREP from every intermediator node (named as an nth node), throughout this case that node which is 1-hop (named as X) before another nth node would be on its real-time mode so it can have overheard the path of the nth node. Thereafter, the X sends the plane packets to the target node via the n node to verify if the nth node forwards the data or not. When the nth node loses plane packets, X sends an alert to all of the other nodes to warn them that there is still a suspicious node in the network, or else the nth node is an old faithful node.

C. Proposed Algorithm

```
EVENT Node "SN" have node data "Da"
Step 1: The sender node sends RREQs to those intermediator neighbors.
Step2: Sender received the RREP packets.
Step3: whether (the RREP packets came from the target node directly) or (Target node is in the direct transmitting radius of the Sender node).
    {
    Sends all of the data (Dt) to this node; //The path is presumed to be secure.
    }
Step4: Otherwise, if the RREP came from any intermediator node
{
If ($L_{tt} < T_t$) then
The node represents as a suspicious node;
Reject this path & send few Warning packets to every intermediator node to separate this suspicious node from the network;
Else
     The node represents as a trustable node; // The path is presumed to be secure
     Send data packets through this path;
}
Step 5: End
```

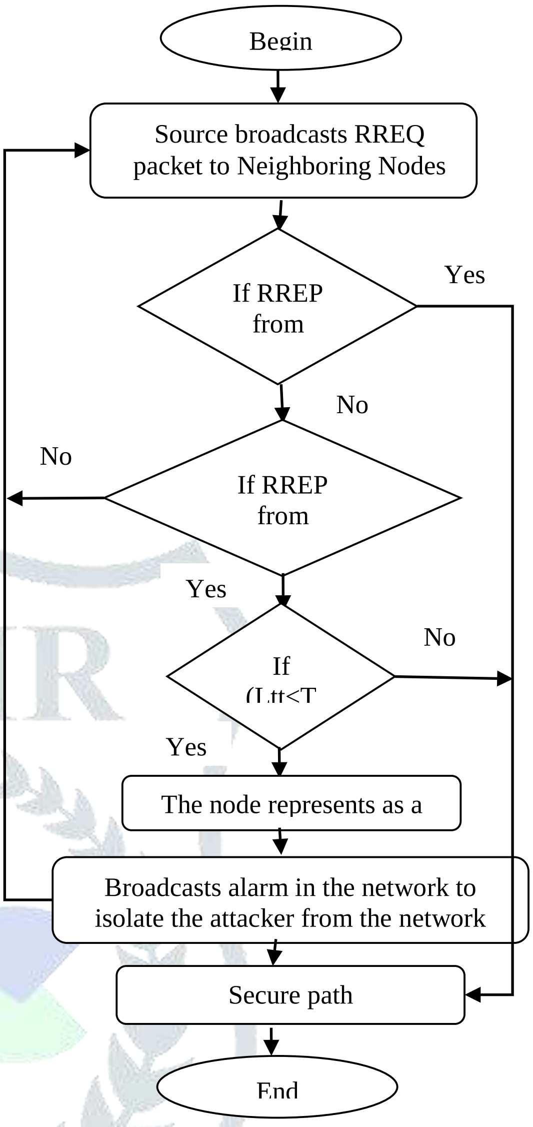
Begin
Source broadcasts RREQ packet to Neighboring Nodes
If RREP from
Yes
No
If RREP from
No
Yes
If (Ltt<T
No
Yes
The node represents as a
Broadcasts alarm in the network to isolate the attacker from the network
Secure path
End

Fig. 2. Flowchart for Detection of the black hole

V. Result Analysis

We have used NS2 simulating tool. We use CBR, UDP/IP, IEEE 802.11b MAC & a physical channel based on a statistics propagation model for performing the simulation. The simulation network includes 20, 30, 40, and 50 at random allocated wireless nodes in an 800 by 800 m^2 plane area.

Table I. List of Parameter specification

Parameter	Value
Simulating time (in seconds)	10
Simulating region (in meter)	800 ×800
Number of nodes	20, 30, 40, 50
Max. size of segments (in byte)	512
Data rate (in Mbps)	Two
Communication radius (in meter)	250
Type of traffic	Constant bit rate
Mobility	Random-way-point

A. Simulation for packet rate without Black Hole Attack in AODV

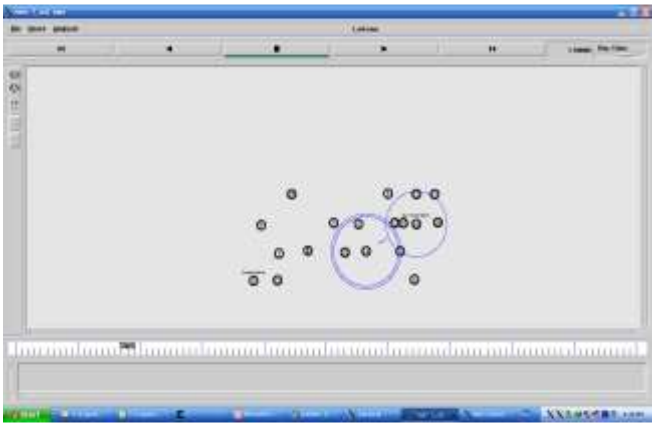

Fig. 3. Simulation for Packet rate without any blackhole node in AODV

In figure 3 were no blackhole attacks in AODV. In this simulation there are the 20 nodes, create a connection between Node 0 and Node 16 where node 0 is a sending node and node16 is receiving node at the simulating animator by NAM. The sending node sends the data packets via node 1, 2, 6, and 10 to the receiving node 16.

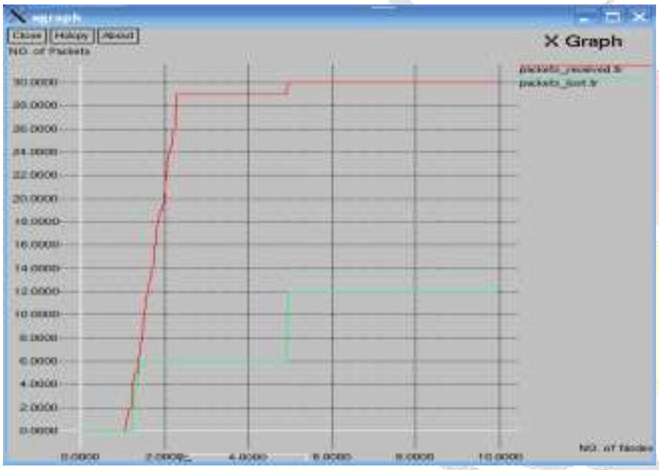

Fig. 4. Packet rate without any blackhole node in AODV

In figure 4 result between two parameter packets received and packet lost. In AODV most of the packets are received as compared to packet lost because in this figure there is no black hole node. In X-axis there are no. of nodes & the Y-axis no. of packets. In node 40 packet received 280 and the packet lost 60. So most of the packets are received in AODV without a black hole attack.

B. Simulation for packet rate with the Blackhole Attack in the AODV

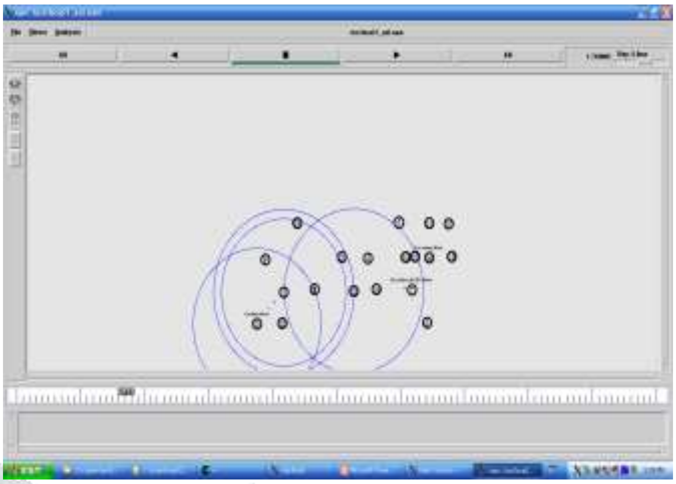

Fig. 4. Simulation for Packet rate with the blackhole node in the AODV protocol

There's also a black hole Node in the AODV shown in Figure 4. In this simulation there are 20 nodes, create a connection between Node 0 and Node 16 where node 0 is a sending node and node16 is receiving node at the simulating animator by NAM. If sending node sends the data packet via node 1, 2, 6, and 10 when the data packet comes to node 7 it may drop all the data packet come to the sending nodes. Because node 7 is the black hole node it drops all the packet.

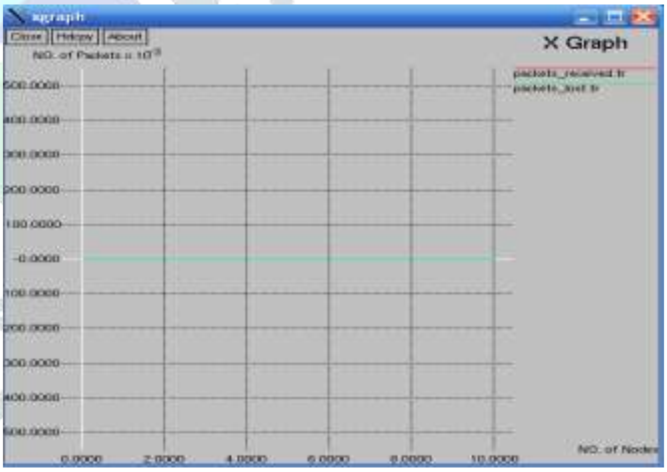

Fig. 5. Packet rate with black hole node in AODV

In figure 5 results between two parameter packets received and packet lost. In AODV there is a blackhole node, so it may drop all the data packet which may come to the sending node or via node1, node 2, node 6, and node 10. Because in the previous figure node 7 is the black hole. So in this figure, all data packet has been lost because there is one black hole node.

C. Simulation for packet rate with Black Hole Attack in Proposed IDSAODV

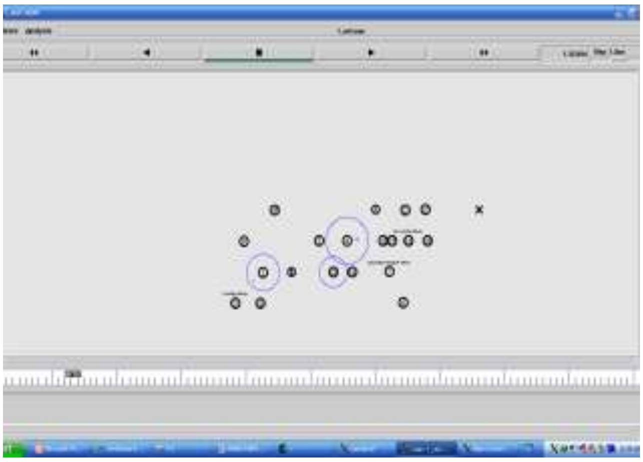

Fig. 6. Simulation for packet rate with black hole node in IDSAODV

In figure 6 shows the blackhole node detection, thus we send the packet to another path which may be safe because in the proposed algorithm wait the second RREP packet then calculates the minimum time. Compare the first RREP time and the second RREP time which is the minimum that node is a black hole node.

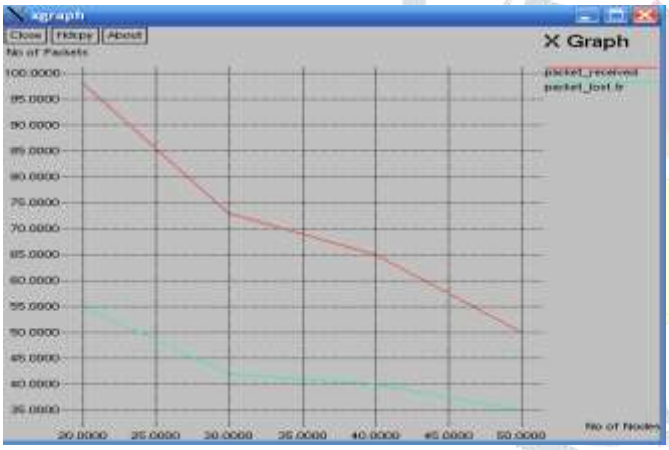

Fig. 7. Packet rate with black hole node in IDSAODV

In figure 7 results between two parameter packets received and packet lost. In IDSAODV detect the black hole node. So when detecting the black hole waiting for the second RREP, when the second RREP has come to the sending node then we calculate the first RREP or second RREP time which is the minimum then send it to the data packet to secure the path. In this figure calculate packet received and packet lost with black hole attack, the packet received as much more than the packet lost.

Table II. Simulation results for a packet received Throughput in AODV protocol with no Blackhole Attack

S. No.	Node Mobility (mps)	Throughput in the AODV protocol with no blackhole attack (%)
1.	20	95
2.	30	78
3.	40	66
4.	50	57

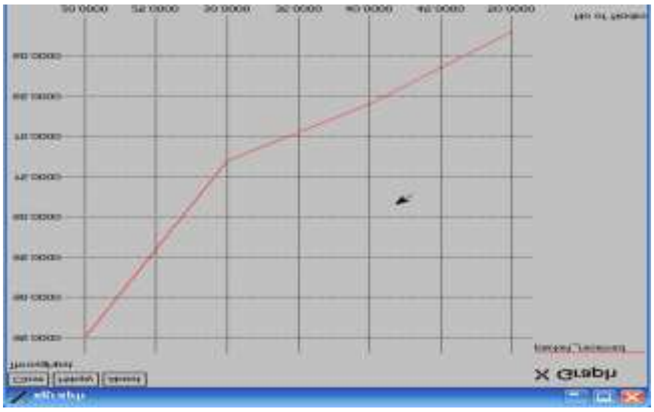

Fig. 8. Packet received throughput in AODV without black hole node

In this figure 8, most of the packets are received in AODV without blackhole attack, because there is no one blackhole node. To calculate the throughput between 20, 30, 40, and 50 nodes. In node 20 throughputs are 95, node 30 throughputs are 78, node 40 throughputs are 66, and node 50 throughputs are 57.

Table III. Simulation results for packet lost Throughput in the AODV protocol with the Blackhole Attack

S. No.	Node Mobility (mps)	Throughput in the AODV with the blackhole attack (%)
1.	20	50
2.	30	42
3.	40	27
4.	50	19

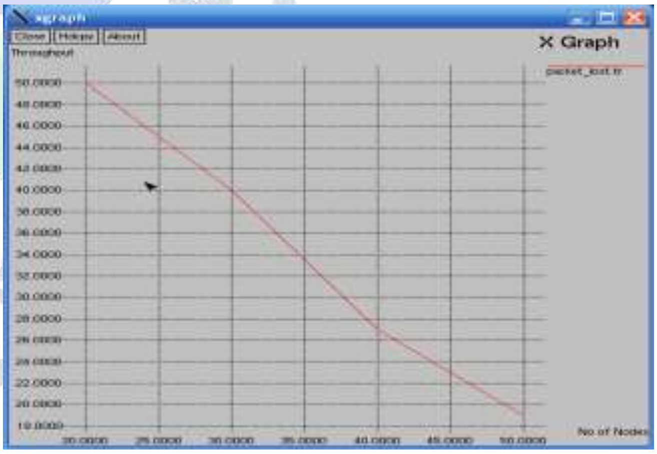

Fig. 9. Packet lost throughput in the AODV protocol with the blackhole node

In figure 9 most of the packets have been lost in the AODV with blackhole node because when creating a blackhole node in the AODV, the blackhole node has dropped all of the packets which come to the sending node. To calculate the throughput between 20, 30 40, and 50 nodes. In node 20 throughput is 50, node 30 throughput is 42, node 40 throughput is 27, and node 50 throughput is 19.

Table IV. Simulation results for a packet received and packet lost Throughput in proposed IDSAODV with Black Hole Attack

S. No.	Node Mobility (mps)	Throughput in AODV with the blackhole attack (in %)	Throughput in proposed IDSAODV with the blackhole attack (in %)
1	20	50	94
2	30	42	72
3	40	27	64
4	50	19	48

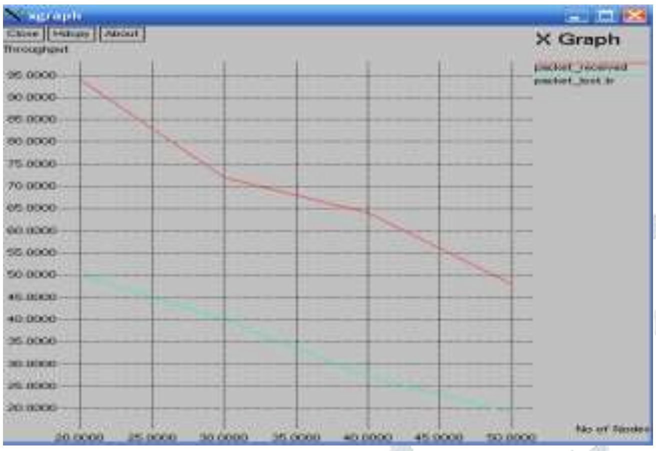

Fig. 10. Packet received and Packet lost Throughput in Proposed IDSAODV with black hole node

In figure 10 calculate the throughput between AODV with the blackhole node & the proposed algorithm with the blackhole node. So packets are received more than the packet lost because in the proposed algorithm check the second RREP time, it may drop that path which time is minimum and send the data packet to the secure path.

Table V. Comparison of throughput outcomes

S. No.	Node Mobility (mps)	Throughput in the AODV with no blackhole attack (%)	Throughput in AODV with the blackhole attack (%)	Throughput in proposed IDSAODV with the blackhole attack (%)
1.	20	95.0	50.0	94.0
2.	30	78.0	42.0	72.0
3.	40	66.0	27.0	64.0
4.	50	57.0	19.0	48.0

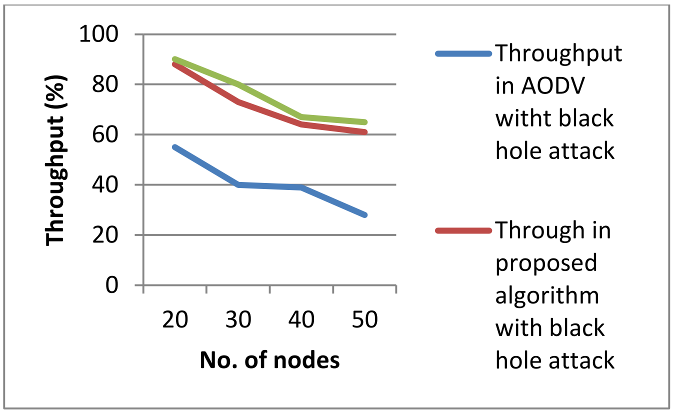

Fig. 11. Throughput in AODV protocol with or without blackhole and proposed IDSAODV with blackhole attack

The effect of the blackhole attack on the network throughput as shown in figure 11 The network throughput is limited due to the effect of the blackhole, but the suggested IDSAODV algorithm offers a better throughput for a blackhole attack.

Table VI. Simulation results for a packet received E2E delay in the AODV protocol with no Blackhole Attack

S. No.	Node Mobility (in mps)	E2E delay in the AODV with no blackhole attack (sec)
1	20	.080
2	30	.131
3	40	.129
4	50	.187

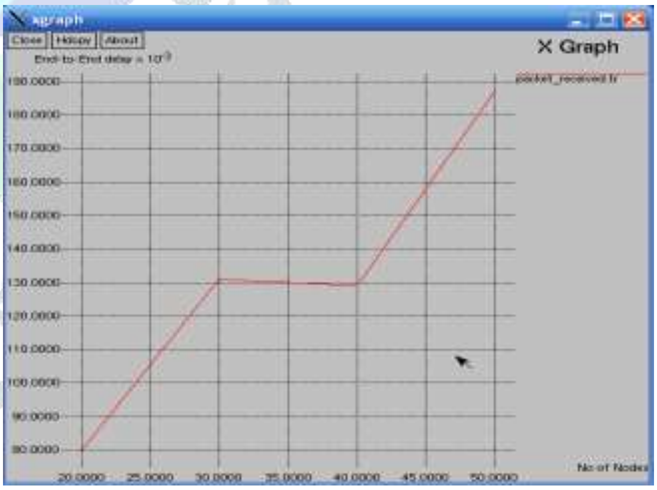

Fig. 12. Packet received for E2E delay in the AODV protocol with no blackhole node

In this figure 12, most of the packets are received in AODV without blackhole attack, because there is no one blackhole node. To calculate the End to End delay between nodes of 20, 30, 40 & 50. In node 20 E2E delay is .80, node 30 end to end delay is .131, node 40 E2E delay is .129 & node 50 E2E delay is .187.

Table VII. Simulation results for packet lost E2E delay in the AODV protocol with the Blackhole Attack

S. No.	Node Mobility (mps)	Throughput in the AODV protocol with the blackhole attack (sec)
1	20	.055
2	30	.112
3	40	.123
4	50	.101

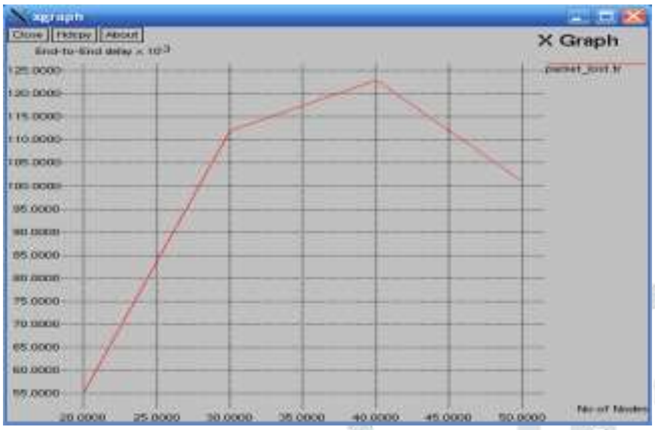

Fig. 13. Packet lost for E2E delay in the AODV protocol with the blackhole node

In figure 13 most of the packets are lost in AODV with black hole node because when creating a black hole node in AODV, the blackhole node dropped all of the packets which come to the sending node. So calculated the E2E delay between nodes of 20, 30 40 & 50. In node 20 E2E delay is .55, node 30 E2E delay is .112, node 40 E2E delay is.123 & node 50 E2E delay is .101.

Table VIII. Simulation results for a packet received and packet lost E2E delay in the proposed IDSAODV with the Blackhole attack.

S. No.	Node Mobility (mps)	E2E delay in the AODV with the blackhole attack (sec)	E2E delay in the proposed IDSAODV with the blackhole attack (sec)
1	20	.055	.100
2	30	.112	.140
3	40	.123	.154
4	50	.101	.202

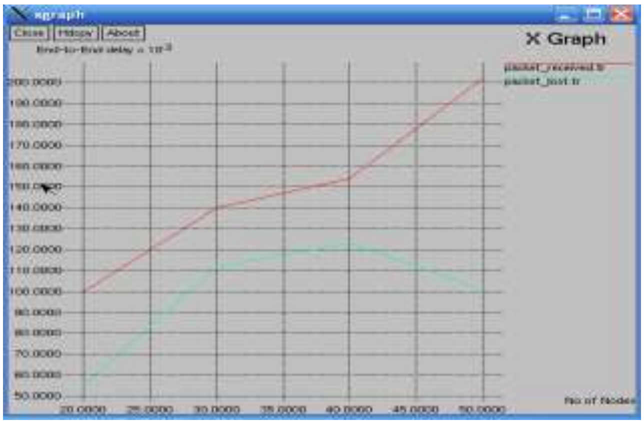

Fig. 14. Packet received and packet lost End-to-End delay in proposed IDSAODV with black hole node

In figure 14 calculate the E2E delay between AODV with the blackhole node & the proposed algorithm with blackhole node. So packets are received more than the packet lost because in the proposed algorithm check the second RREP time, it may drop that path which time is minimum and send the data packet to the secure path.

Table IX. Comparison simulation results of E2E delay

S. No.	Node mobility (mps)	E2E delay in the AODV with no blackhole attack (sec)	E2E delay in the AODV protocol with the blackhole attack (sec)	E2E delay in proposed IDSAODV with the blackhole attack (sec)
1.	20	.080	.053	.100
2.	30	.131	.112	.140
3.	40	.129	.123	.154
4.	50	.187	.101	.202

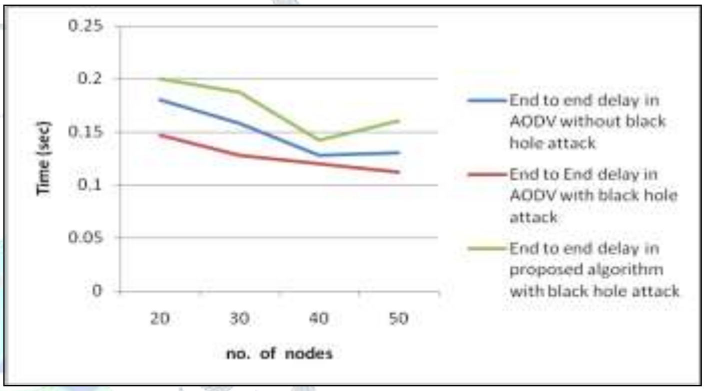

Fig. 15. E2E delay in the AODV protocol with or without blackhole and proposed IDSAODV with the blackhole node.

From figure 15, it could be seen that there is a small improvement in the avg. E2E delay with no impact of the blackhole opposed to the impact of the blackhole attack, which is linked to the instant response of the suspicious node, that is the essence of the suspicious node here is that it would not search in its routing table.

VI. Conclusion

The MANET is a self-configured infrastructure-less network for mobile systems. Every one of them should forward traffic irrelevant to their usage, and thus be a router. AODV is a loop-free routing algorithm for an Adhoc network. It is built to be self-initiative in a mobile node system, taking into account a set of network activities, along with node mobility, connection failures, and so on. Black Hole Attacks is a type of DoS attack during which a router which is meant to relay packets dropped them afterward. AODV routing protocol is used in this paper. We shadowed the five 20-node scenarios consuming AODV protocol as well as following the same scenarios after the black hole node in the grid. Our simulation results have been analyzed. After mimicking the black hole attack, we have seen an enhances in the packet loss in an allocated network. The simulation result table shows the difference between the blackhole attack and lost packages on the network. networking parameters such as Throughput, Packet transferring rate & avg. E2E delay has been measured for a normal network (with no blackhole) and even a single blackhole network. Since the blackhole attack has been found in an attempt to maintain data transfer, the blackhole node is avoided, and also the path to the actual target is redirected. n all 3 cases, the efficiency of the networking parameters has compared. The findings have shown that the proposed IDSAODV protocol can be highly defended against all the blackhole attack that happens mostly during the forwarded process.

Research may also be applied to secured routing protocols against all other attacks including Gray Hole Attack, Wormhole Attack, and so on. Such attacks can be classified mostly on the principle of the degree to which they influence the efficiency of the network. Even several routing protocols including DSR, TORA, etc. may also be simulated. Both routing protocols are supposed to yield different effects. The effective routing protocol for mitigating the Blackhole attack may therefore be calculated.

References

[1] Ashwini S Hosgouda and Prof. M.S Shobha, “A Survey on Black Hole Attack Detection in MANET Using AODV Protocol”, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.1, January- 2015, pg. 415-420.

[2] Fan-Hsun Tseng, Li-Der Chou & Han-Chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", Human-centric Computing and Information Sciences, volume 1, Article number: 4 (2011), pp. 1-16.

[3] Vinay Singh, Dr. Ajit Singh, and Malik Mubasher Hassan, "Survey: Black Hole Attack Detection in MANET", 2 nd International Conference On Advanced Computing and Software Engineering (ICACSE-2019), pp. 522-525.

[4] Mohite, V. G., & Ragha, L., “Security agents for detecting and avoiding cooperative blackhole attacks in MANET”, 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), 2015, pp. 306-311.

[5] M. Y. Dangore and S. S. Sambare, "Detecting and Overcoming Blackhole Attack in AODV Protocol," 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies, Pune, 2013, pp. 77-82, DOI: 10.1109/CUBE.2013.23.

[6] FIHRI Mohammed, OTMANI Mohamed and EZZATI Abdellah “The Impact of Black-Hole Attack on AODV Protocol”, (IJACSA) International Journal of Advanced Computer Science and Applications, Special Issue on Advances in Vehicular Ad Hoc Networking and Applications, 2014, pp. 20-24. DOI: 10.14569/SpecialIssue.2014.040204.

[7] S. Shrestha, R. Baidya, B. Giri and A. Thapa, "Securing Blackhole Attacks in MANETs using Modified Sequence Number in AODV Routing Protocol," 2020 8th International Electrical Engineering Congress (iEECON), Chiang Mai, Thailand, 2020, pp. 1-4, DOI: 10.1109/iEECON48109.2020.229555.

[8] A. M. El-Semary and H. Diab, "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map," in IEEE Access, vol. 7, pp. 95197-95211, 2019, DOI: 10.1109/ACCESS.2019.2928804.

[9] Qussai M. Yaseena and Monther Aldwairi, “An Enhanced AODV Protocol for Avoiding Black Holes in MANET”, Procedia Computer Science 134 (2018) 371–376.

[10] G. Bendale and S. Shrivastava, "An improved blackhole attack detection and prevention method for Wireless ad-hoc Network," *2016 International Conference on ICT in Business Industry & Government (ICTBIG)*, Indore, 2016, pp. 1-7.

[11] P. R. Dumne and A. Manjaramkar, "Cooperative bait detection scheme to prevent collaborative blackhole or gray hole attacks by malicious nodes in MANETs," *2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, 2016, pp. 486-490.

[12] Kumar, V., & Kumar, R. (2015). An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network. Procedia Computer Science, 48, 472–479.

[13] H. P. Singh and R. Singh, "A mechanism for discovery and prevention of cooperative black hole attack in mobile ad hoc network using AODV protocol," *2014 International Conference on Electronics and Communication Systems (ICECS)*, Coimbatore, 2014, pp. 1-8.

[14] P. N. Patil and A. T. Bhole, "Blackhole attack prevention in mobile Ad Hoc networks using route caching," *2013 Tenth International Conference on Wireless and Optical Communications Networks (WOCN)*, Bhopal, 2013, pp. 1-6.

[15] D. Kshirsagar and A. Patil, "Blackhole attack detection and prevention by real-time monitoring," *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, Tiruchengode, 2013, pp. 1-5.

[16] P. K. Singh and G. Sharma, "An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET," *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, Liverpool, 2012, pp. 902-906.