IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# SECURING BLACKHOLE ATTACKS IN MANETS USING MODIFIED SEQUENCE NUMBER IN AODV ROUTING PROTOCOL

**Ramya kulkarni**
Department of MCA,
VTU's CPGS, Kalaburagi, India.

**Ambresh Bhadrashetty**
Assistant Professor,
Department of MCA,
VTU's CPGS, Kalaburagi, India

***Abstract*—Private Cellular Network (MANET) is a structure distributed among mobile nodes, which enables information to be shared without the need for infrastructure Nonetheless, due to the lack of a single regulatory authority; MANETs suffer a range of security problems, in contrary to its infrastructure-based equivalents. One of most difficult security challenges with MANETs is the black hole attack. Source and target interrupt data flow a black hole attack significantly lowers efficiency of the network. We propose a method in this work that Technology based on change hash value contained In the case of holding, namely Forward reply packet (RREP) in common protocols The Ad-Hoc on Demand Distance Vector (AODV) routing protocol is used to identify black hole nodes, thereby reducing data loss by rerouting the routes of these nodes. Our suggested approach outperforms current traditional Interruption Detection System (IDS) provided for AODV, as according simulation results.**

***Keywords—Blackhole attack; AODV; IDS; Sequence Number***

## *1.INTRODUCTION*

Ad-hoc networks are unstable connections that occur spontaneously between hubs. It doesn't depend upon any prior

foundations like switches, passages or base stations. Singular hubs associated with this sort of organizations can advance parcels to and from one another when they exist in one another's scope of transmission. When the portable hub started such an organization, it was called the Mobile Ad-hoc Network (MANET). In the absence of a major regulatory agency that manages licenses, any available center within the organization can easily become interested in MANET. Ultimately, the security in MANET is powerless. Receiving communications between different centers will eventually cause many security threats. One of such security issues is black hole assault. Black hole assault specifically influences the organization layer execution. A hub going about as black hole drops the information bundles as opposed to transferring them to some other hub set apart as objective hub. In a black hole assault, a hub publicizes itself as the hub with most ideal course, for example a next bounce hub having a new way with the least jump tally to the objective hub. All things considered, well known steering convention like AODV,

then again, incline toward the course with least jump check and most extreme succession number.

## 2. VULNERABILITIES IN MANETS

Keeping all the convenience aside, the properties of MANETs are such that security is always going to be an issue. These vulnerabilities can be simply put as listed below [8].

A.Wireless Links

Unlike wired networks, wireless connections can be used for all other devices on the network, making wireless connections vulnerable to security issues.

B. Dynamism

Nodes in MANET can move freely, join or leave the network,resulting in frequent changes in the network topology. Therefore, there is no guarantee that the package has been delivered or legal. The road will lead to the destination.

C. Cooperativeness

In MANET, the routing algorithm assumes that all nodes trying to join the network are not malicious and can help route data packets through the network. On the other hand, trust in the MANET algorithm can easily be broken. It is easy to cause network interruption.

D. No central authority

According to the definition of MANET, there is no central authority to supervise the overall operation of the network or monitor any rogue nodes that may exist.

## 3. RELATED WORKS

Although MANETs are increasingly popular, their security issues have been ever present since they have come into consideration, including problem of blackhole attack. To address the problem, some schemes have already been proposed.

- Intrusion Detection System (IDS)

Fu H. et,al. suggested a solution known as IDS based on the assumption that a malicious node, in an attempt to present itself as the most viable option, replies with a RREP packet as soon as it receives the RREQ packet. It further assumes that the source node receives the first reply from the malicious node with highest probability. So IDS, considering the node replying with the first RREP as a malicious node, suggests to discard the first RREP received by the source node, and instead use the route corresponding to the RREPs received later on [6].

- Anti Blackhole Mechanism (ABM)

ABM, a solution to blackhole in MANETs, proposed by M. Y. Su et.al., suggests the use of an additional parameter called suspicion value which shall be assigned to every node willing to take part in the data transmission. A prerequisite set by ABM is such that, every node in the network should previously have generated a RREQ for a destination node before it could reply with a RREP packet for the same. In case this condition is not met, the suspicion value for that node is incremented. A threshold value for suspicion is then set, so as to declare a node to be malicious i.e. if the threshold value of suspicion of any node is exceeded then it is declared to be malicious. [7]

## 4. PROPOSED ALGORITHM

Considering the above mentioned issues and the available solutions, in this paper a new approach has been suggested to address the problem of blackhole. It is known that a blackhole node attempts to appear as the most favorable next hop node for the source node to reach the destination node. It does so by replying with a RREP packet with false information of having the least hop count and the highest sequence number, respectively where, hop count denotes the number of nodes between the sender and receiver node in a route and sequence number shows the freshness of the route. Thus taking these behaviors into consideration, in this algorithm, we assume that the attacking node increases the sequence number in the RREQ packet by an arbitrary maximum number ( Arbtmax ) of 100, when replying. The Arbtmax value is considered to denote abrupt or suspicious rise in sequence number denoting routes between the mobile nodes. The suggested solution attempts to exploit this characteristic of a blackhole node and then makes provision of a technique in which a source node double checks the validity of the intermediate node that replies with an RREP packet having destination sequence number suspiciously high. When a source node receives a RREP packet having a destination sequence number greater than the source sequence number by more than the assumed Arbtmax , it rebroadcasts the RREQ packet but this time with the destination sequence set equal to the sequence number of the received RREP packet. If a RREP packet is again received with suspiciously high destination sequence number from same node then the path is discarded. Pseudo Code of Proposed Algorithm Notations SN: Source Node IN: Intermediate Node RRq: Re-Broadcast RREQ SSN: Source Sequence Number DSN: Destination Sequence Number Mal: Malicious Node

1. SN Broadcast RREQ

2. Wait for RREP

3. On Receiving RREP

4. IF (RREP Sequence Number –SSN> max Arbt ) {

5. RRq by changing SSN to RREP sequence number

6. Wait for RREP

7. IF (RREP Sequence Number – SSN > max Arbt ) {

8. Mal Detected

9. Discard the Route

10. }

11. }

12. ELSE {

13. Send the Data Using the Route

14. }

## 5. PERFORMANCE ANALYSIS

For validating the suggested algorithm, a series of simulations was performed in Network Simulator-2 (NS2). Table I lists out the simulation parameters in detail. The performance of the proposed algorithm is compared with the IDS AODV and AODV protocol respectively in the presence of blackhole nodes in reference of 100 simulations in the NS-2 platform. Further, the simulation parameters are also varied in terms of the nodes present in the network. Throughput and Packet Delivery Ratio are considered to be the performance metrics. Throughout the series of simulations only a pair of source and destination nodes are considered. Simulations are performed in two different network configurations as follows:

• The number of mobile nodes in the network are varied from 10 to 50 where 5 blackhole nodes are constantly present.

• The number of mobile nodes is set to 30 while changing the number of blackhole from 1 to 10.

The results presented in Fig. 1 to Fig. 4 are generated from the average value of the varying data related to the performance metrics obtained over 100 simulations. The variation in the data after each simulation is due to the random mobility of the nodes present in the network and the dynamic network topology.

TABLE I : SIMULATION PARAMETERS

| Parameters | Details |
|---|---|
| Simulation Dimension | 500 x 500 |
| Simulation Duration | 100 Seconds |
| Node Density | 10 to 50 Nodes |
| Malicious Node | 1 to 10 Blackhole Nodes |
| Movement/Position | Random |
| Routing Protocol | AODV, IDS AODV, Proposed Algorithm |
| MAC | MAC 802 11 Ext (IEEE 802.11p) |
| PHY | PHY Wireless 802 11 Ext (IEEE 802.11p) |
| Propagation Model | Two Ray Ground |
| Antenna Type | Omnidirectional |
| Transport Layer | UDP |
| Traffic Model | CBR |

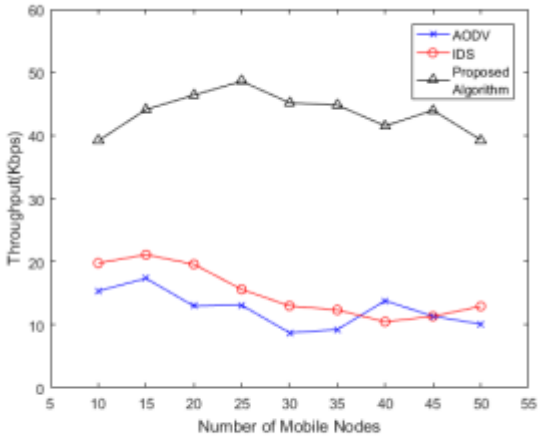


*Fig 1: Throughput Performance in Presence of five Blackhole Nodes*

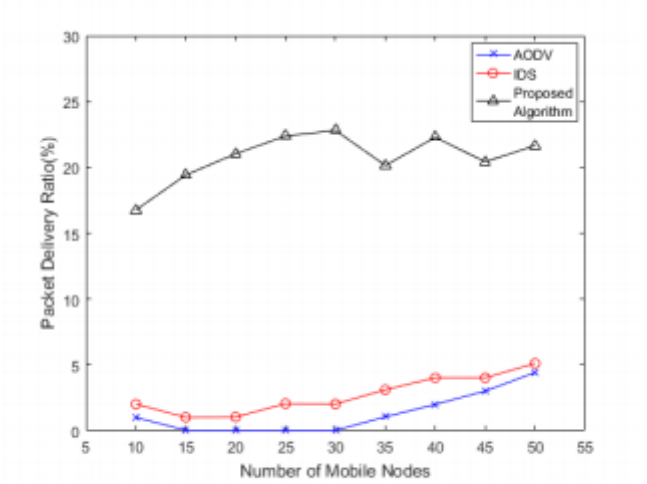


*Fig 2: Packet Delivery Ratio in presence of five Blackhole nodes*

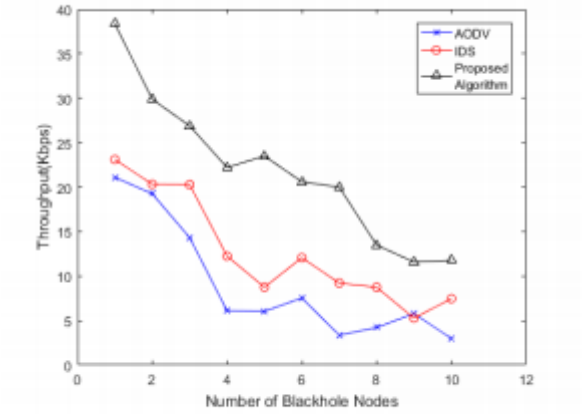


*Fig 3: Throughput Performance in presence of thirty mobile nodes*

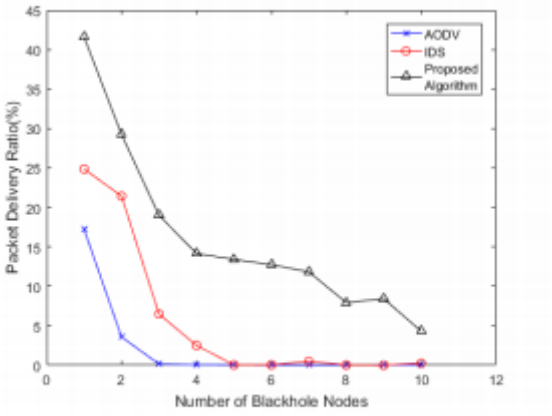


*Fig 4: Packet Delivery Ratio in presence of thirty mobile nodes*

Figure 1 shows the performance of the network in terms of throughput when 5 blackhole nodes are constantly present in a network of varying number of mobile nodes. Since the number of blackhole nodes is constant for this set of simulations the throughput seems to be increasing as the total number of mobile nodes increases. However, as the number of nodes increases there comes a point where the throughput reaches saturation and then starts to decrease. In all cases the proposed algorithm performs better than the available algorithms.

Figure 2 indicates that the packet delivery ratio goes on increasing as the number of participating nodes increases and here as well the performance of the proposed algorithm can be noticed to have better result. In Fig. 3 when blackhole nodes start to increase the throughput starts to decrease as the number of packet drop starts to increase. However, in all the cases the performance of the proposed algorithm is better than the legacy ones. Similarly, in Fig. 4 the packet delivery ratio goes on decreasing as the number of blackhole nodes increase due to higher packet drop probability. Nevertheless, the performance of the proposed algorithm is higher in all the scenarios as well. Thus it can be clearly seen that the proposed algorithm attempts to address the problem of blackhole in MANETs in a simplistic yet effective way. Upon the usage of the suggested algorithm we can hence expect a better performance.

## *6. CONCLUSION*

This paper presented the study of a security issue named blackhole in MANETs and discussed its impact on the network. Also, the existing solutions to the issue are studied, analyzed and based on that a new algorithm is proposed. The proposed algorithm is very simple and can perform well in comparison to the legacy algorithms. The validity of the proposed algorithm is also checked through network simulation.

## *7. REFERENCES*

[1] K. Xu, X. Hong and M. Gerla, "An ad hoc network with mobile backbones," in IEEE International Conference on Communications, 2002.

[2] H. Deng, W. Li and D. P. Agrawal, "Routing security in wireless ad hoc networks," IEEE Communications Magazine, vol. 40, no. 10, pp. 70-75, 2002.

[3] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination- Sequenced Distance Vector Routing(DSDV) for Mobile Computers," IETF, 1994.

[4] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc," in Mobile Computing, vol. 5, C. P. Perkins, Ed., Kluwer Academic Publishers, 1996, pp. 153-181. [5] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, 1999.

[6] H. Fu and H. Weerasinghe, "Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation

implementation and evaluation," Future Generation Communication and Netwroking, vol. 2, pp. 362-367, 2007.

[7] M. Y. Su, "Prevention of selective blackhole attacks on mobile ad-hoc networks through intrusion detection system," Computer Communications, vol. 34, no. 1, pp. 107-117, 2011.

[8] M. Fihri, M. Otmani and A. Ezzati, "The Impact of Black-Hole Attack on AODV Protocol," International Journal of Advanced Computer Science and Applications, Special Issue on Advances in Vehicular Ad Hoc Networking and Applications , pp. 20-24, 2014.