To Detect and Isolate Black Hole Attack in MANET Using AODV (ADHOC on Demand Distance Vector Routing)

MANU DEVI, Manu Ghanghas

UIET, MAHRISHI DAYANAND UNIVERSITY, ROHTAK, HARYANA

Abstract
Adhoc network is a kind of multiple node wireless network which works on variable nodes. A mobile adhoc network may be connected to other fixed network and to the Internet. Mobile Adhoc Network (MANET) have the preservative functionality and huge no of security threat. Because of dynamic characteristics and addictive functionality, the network suffers various form of attacks. Black hole could be loophole in routing which damage the network. Black hole part is that part in network where sending or receiving packet discarded without giving the data to sender that data fail to reach to the receiver. Black hole route could be a network-route in routing table entry that goes nowhere. Identical packet is discarded acting as firewall having limited capacity. During this technique, the secure mechanism which is employed for checking the forwarding of packets by intermediate nodes was analyzed. There are numerous methods for discovering black-hole type attacks in wireless Adhoc network like Intrusion detection System, check agents and multiple base stations. AODV protocol for detection of unwanted node.

Keywords:
MANET, malicious node, Constant Bit Rate (CBT).

1. Introduction

Wireless network is infrastructure less wireless network which goes famous because of its environmental condition and better performance. It's a centralized network of devices that accustomed to communicates for information gathering through wireless path. Node in wireless network sending data through multiple hops, gateway, the information is connected through other network like wireless Ethernet. Wireless network is becoming extremely popular because of its performance, scalability to large scale of distribution, cross layer design. Security being a significant issue, the nature of adhoc network makes them very easy. Mobile adhoc network doesn't relay on the permanent existing infrastructure. MANET may be a collection of independent (KUMAR, 2009)mobile that may communicate with this node via radio wave. In MANET the participating node acts as a router which may be unengaged to move randomly and can have arbitrary management. Routing is that the important part in networking. The aim of routing is to seek out the simplest path between the communicating nodes. There are mainly two ways of shorting routing_algorithms in MANET- Reactive protocols and other one as Proactive. Malicious node is the problem for disturbing the correct operation and reduces the performance and throughput of network. Only malicious node is accountable for all attack in MANET. On demand routing strategy creates and maintain path between source to destination and it include discovery of route and route maintenance. Routing is that the process to move about information from one place to a different. In routing two activities are involved. First is to work out optimum path and second is to transfer packet through the network.

Manuscript received April 5, 2025
Manuscript revised April 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.4.8

2. Methodology

Researchers have proposed various techniques to prevent black hole attack in mobile adhoc network. Yibeltal [3] introduces the use of REWARD to detect counter attack against single node or team of malicious node (link).This algorithm is suitable for network nodes that can tune their transmit power. This algorithm utilizes the broadcast message to organize database for detecting black hole. The main drawback of this algorithm is that it has different level of security which can be set according to local condition and due to limited enery resources no alternate power resources energy overhead. In counter algorithm approach used for security and prevention in AODV routing, source node without changing intermediate node and destination node by using a receive- reply message. This method works only for source and destination node there is no involvement of intermediate node. In this only sequence no. checking technique used.

3. AODV Routing

In reactive approach, path to receiving node is not established until we have data packet to transmit. AODV is a routing protocol for MANET and other wireless adhoc network. AODV is using multiple technologies based on Distance Vector Routing. In AODV there are three kinds of packets that are used for path discovery and path maintenance. These are REQ, RREP and R_RER. During route discovery, sender broadcast a RREQ message which

contain IP address and last sequence no. of receiving node. This message is received by every neighbor node. This node checks whether they are destination or have route for destination. If not RREQ message is received by destination node of node which having path for destination, it will generate RREP and unicast it back to source node. When the node receive RREP route discovery is complete and then sender start to send packet to destination via path. If any path or link broken then R_RER message broadcast to all node for route updation [7].

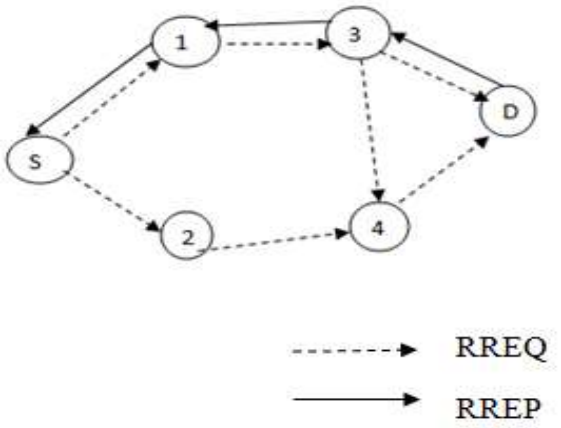


Figure 1 AODV Route Discovery.

In Figure 1, when sender wants to send the data to receiver it check its routing table, if routing table entry is found then it send to destination otherwise it starts path discovery and broadcast RREQ packet to neighboring node if neighboring node has path to destination they send RREP to sender otherwise forward to next node. When destination or neighbor receive RREQ then it send RREP to source, after receiving RREP it start sending data to destination.

4. Black Hole Attack

In black hole effect, when the RREP message is sending by source node and this message is received by malicious node it will generate a fake RREP and put long destination sequence no. filed and unicast to sender.When source node receive RREP the sender start to forward the data to malicious node assuming that it is the shortest for sending the data to destination and by ignoring other RREP packet. The data packet received by malicious node not forward by any other node is called black hole attack. (Dimpal Joshi*1, 2018)

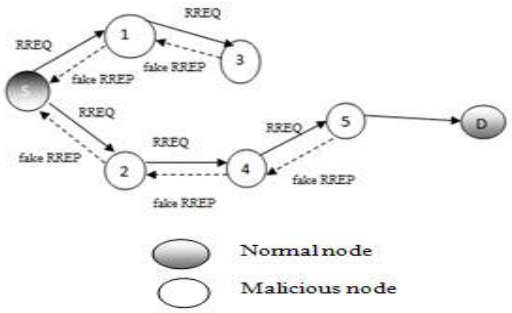


Figure 2 false RREP send by malicious node

In the Figure 2, the sender wants to communicate with receiver for which it broadcast RREQ message. But node 2 and 5 are malicious node unicast fake RREP to source node and when sender starts forwarding the packet to them they dropped the data packet. The detection of black hole can be possible in AODV routing protocol. In this a type of trap method is implemented.

5. Proposed Work

In this research detection of malicious node change functioning without involvement of intermediate malicious node. The AODV routing mechanism will be implemented by using the following steps:

Step1: First of all we have to search out that Data packet which is coming from malicious node.
Step2: Next step is to check what no. Requests are coming from each node in what quantity time.
Step3: removing malicious node from malicious node list after the session expired. We should always remove malicious node and forward route request.

Algorithm:

```
When RREQ request from neighboring node
Step: 1 Is node in node list
{
If yes, then send route request
}
Else move to step 2
Step2: node in RREQ Table
Yes
If(RREQ> max_RREQ)
{
Add in malicious list
}
If( node RREQ time expire<=current time)
{
RREQ table delete
}
Else continue AODV process
No
RREQ entry in RREQ table
{
RREQ time expire=current time+waiting time
RREQ=1
}
Step 3: time handler
If(malicious node time<=current time)
{
Remove node from malicious list
}
Then
Step 4: continue AODV process.
```

The complete process of the AODV algorithm will be understood by using the flow chart which is shown below:

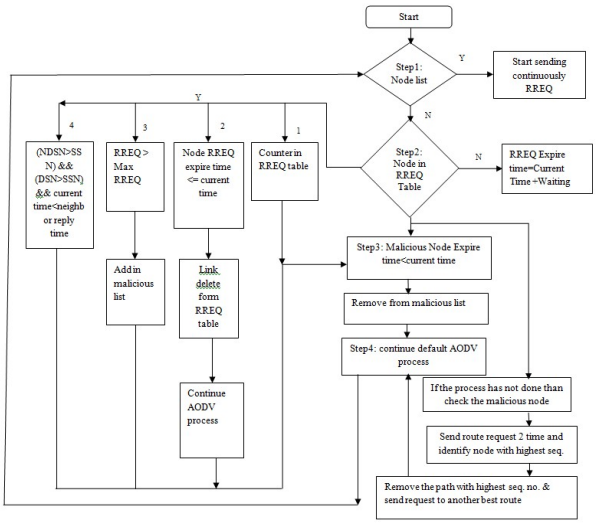


Figure 3 AODV algorithm

6. Results

In the table some parameter are used for create topology.

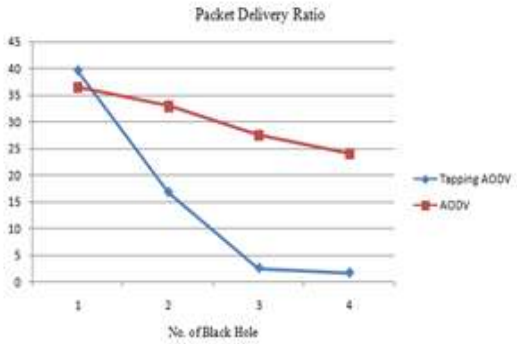
Table1: Parameter used in implementation

Parameter	Value
Simulator	NS2
No. of nodes	30,35,40
Time	100s,200s
ApplicatinTraffic size	CBR(constant Bit Rate
Packet size	512 bytes
Routing Protocol	AODV
Maximum Speed	1m/s
Maximum bandwidth	2Mbps
Black hole node	1-4

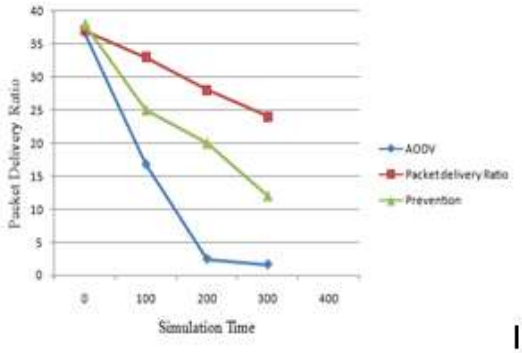
Performance Matrics

Performance Matrics	**Descrptive criteria**
Throughput	Average rate of successful packet delivery; Throughput=Total received Packet/ Simulation time.
Packet delivery Ratio	It is the ratio of packet received at receiver end to the packet delivered at sender end. Packet Delivery Ratio= Packet Received / Delivered Packet

No. Of Black hole	TappingAODV	AODV
1	39.68	36.5
2	16.79	32.92
3	2.509	27.54
4	1.654	24



Graph1: Packet Delivery Ratio



Graph2: Packet Delivery Ratio vs Simulation time

Figure 4 Packet Delivery Ratio and Si,ulation Time

From the above result in Figure 4, it's clear that packet delivery ratio of AODV is best as compared to the other technique because the black hole nodes increase.

7. Conclusion

In this paper, we've analyze an algorithm to reduce the black hole attack and discard the unwanted node. The proposed algorithm reduce malicious node performance without the maximum amount network overhead in term of parameter like end to end delivery, packet delivery ratio etc. Our proposal is to mitigates the effect of black hole and malicious node uses c AODV as routing protocol. Simulation of security strategies provides the facility to select a good solution for routing protocol. As the future work, we might refer to remove other form of attack like denial of service, counter attack, worm hole attack etc. The longer term research should be able to overcome network attack which redue the link breaking problem.

References

[1] Neha sharma, aAnand singh BisenVITM gwalior,india,detection as well as removal of black hole and grey hole attack in MANET, International conference of Electronics and Optimization Techniques(ICEEOT)-2016.
[2] A.Babu Karuppiah,J.Dalfiah, Velammal college of engineering & Technology, Madurai, Chennai, An improvised hierarchical black hole detection algorithm in wsn,India2015ICIICT.
[3] Yibeltal F Alem,Australian National University , Preventing black hole attack in mobile adhoc network using anomaly detection,article January 2020.
[4] Karakehayov Z. Low power communication form wireless adhoc network, ELECTRONICS'2003.
[5] Abderrahmane Baadache, Laboratory of Industrial Technology and Information,Avoiding black hole and cooperative black hole attack in wireless adhoc network,IJCSIS, volume 7,No. 1,2010.
[6] Luka Daoud,and Nader Rafla, Electrical and computer Engineering, IEEE proceeding 2019.
[7] Ming yang su,Ming Chuan university Taiwan, prevention of selective black hole attack MANET using IDS, Elsevier 2010.
[8] Reem Alattas, Department of computer Science and Engineering, Bridgeport, delecting black hole attack in wsn using multiplem base station and check agent, Future technology conference FTC-2106.
[9] Bo sun yong Guan jian chen,department ofd computer science, texax A & M university,the institute of electrical engineers,ichael faraday house, six hill way 2003.
[10] Asmae Blilat, Anas Bouayad, wireless sensor network security challenges,IEEE national days of network security and system JNS2 2012.