Pak. J. Biotechnol. Vol. 13 special issue II **(International Conference on Engineering and Technology Systems (ICET'16) Pp. 62 - 66 (2016)**

ISOLATION OF BLACKHOLE ATTACK IN MANET USING MAODV PROTOCOL WITH CA ALGORITHM

J. Gautam, S. Sindhuja and D. Nagavalli

Department of Information Technology, Velammal college of Engineering & Technology, Madurai, India.
gjp@vcet.ac.in, sindhujass18@gmail.com, dhanamnagavalli@gmail.com

ABSTRACT

Mobile Ad-hoc Network (MANET) is a self-organized system encompassed of mobile nodes without any infrastructure. Security is a decisive requisite in Mobile Ad-hoc Network (MANETs) when accessed to wired networks. Blackhole attack is a arduous issue to be addressed in MANET. Blackhole node falsely claims that it has the shortest path to the destination and dumps the packet that is supposed to be forwarded. In order to reduce the effects of Blackhole attack, we are modifying the AODV protocol and proposing counter attack algorithm that provides a efficient way to mitigate such attacks.

Index Terms— MANET,Blackhole Attack, MAODV, Counter Attack algorithm.

I. INTRODUCTION

A network is a set of devices or nodes connected via communication links. A node can be computer, printer or another device component of sending and receiving information generated through different nodes on the network. Network need to able to meet specific standards they are efficiency, reliability and safety. One of such network is Mobile Adhoc Network. A Mobile Ad hoc network (MANET) is a constantly self-configuring, infrastructure-much less community of mobile gadgets connected wirelessly. Every device in a MANET is free to move independently in any direction, and will thus alternate its hyperlinks to different devices. Every node has got to forward site visitors unrelated to its own use, and thus be a router. They may include one or more than one and different transceivers between nodes. A protocol that is used in MANET is AODV protocol. The AODV protocol builds routes between nodes supplied that they're requested. AODV is thus viewed an on-demand algorithm and does not create any additional visitors for conversation alongside links. In communication using

MANET the major threat is the Blackhole attack. Blackhole attack is without doubt one of the security assault that occurs in MANET. Blackhole node is a node where the incoming and the outgoing data varies wherein a router that's alleged to relay packets instead discards them alongside links.

II. RELATED WORK

Ketan S. Chavda [2] proffered a method in which there are two RREP are compared using compare_RREP. If the result of this comparison is large, then there is a possibility that the node is a malicious node.

Nisha and Samrajit Kaur [3] put forward a way to find the chain of Blackhole node that drops packet fractions. For this, rather than sending total data instantly, the data is divided into blocks of small size. By this, the Blackhole node can be found and mitigated in between the transmission between two blocks by end to end checking. Here the traffic flow will be monitored. By the monitored information, the data loss during transmission is foundout. If the data loss is in tolerable range, then the node can be used.

Rutvij H. Jhaveri [1] proffered a method in which, each node finds a value called PEAK value for some time interval. If the PEAK value is lesser than the sequence number, then it is considered to be a malicious node.

Surana et al., [6] suggested a mechanism that uses promiscuous mode to detect a malicious node during route determination phase and provides an alternate route; it maintains two extra tables pending packet table and node rating table. If packet is not forwarded by adjacent node, the node rating table is updated accordingly.

IrshadUllah and ShoaiburRehman [8] proffered that In Black hole attack, suppose if a node tries to communicate with the other node out of its range then intermediate selfish node will drop its packet. So data gets lost.

Sanjay Ramaswamy et al., [9] proffered a method in which multiple Black holes are seen cooperating with each other and thus discovering a solution for safe route avoiding cooperative Black hole attack.

Nitin Khanna and Priyanka Sharma [5] suggested a mechanism that makes use of color scheme to describe the trust of a node. Identical to visitors gentle this mechanism makes use of three colors to depict the trust.

Kejun Liu et al., [4] proffered a system, in which if there is a routing misbehaviour then there will be two acknowledgement schemes for the misbehaviour and recovering the misbehavioring effects. Here there is a focus on the link in which there is a misbehaviour rather than concentrating on nodes.

Jain, et al., [7] proffered an algorithm to detect a chain of cooperative malicious node in ad-hoc network that disrupts transmission of data by feeding wrong routing information along with the detection algorithm. We also propose a mechanism to detect and remove the black and gray hole attacks.

III. OVERVIEW OF AODV

AODV has pooled properties of both DSR and DSDV. It uses route discovery process for sustaining route information through the basis of routing table. It is a reactive protocol as it doesn't need to establish or maintain routes to nodes that are not involved in the communication. AODV handles route discovery process with Route Request (RREQ) messages to broadcast to neighbour nodes. The message floods through the

network till the desired destination is reached. Sequence number guarantees the loop freedom. The destination node at once receiving a RREQ unicasts a Route Reply (RREP) back to the source node. Node transmitting a RREP message creates routing table entries for forward route. For route maintenance, nodes send HELLO messages intermittently to neighbour nodes. If any node in the network miss the mark to receive three consecutive HELLO messages from its neighbour, it presumes that link to that particular node is down. A node that perceive a broken link directs a Route Error (RERR) message to any upstream node. At once a node receives a RERR message it will signpost a new source discovery process. The AODV protocol uses sequence numbers to determine the timeliness of each packet and to preclude the creation of loops. The route entries are updated by expiry timers. Link failures are propagated by a route error (RERR) message from a broken link to the source node of the corresponding route. As soon as the next hop link breaks, RERR packets are sent by the introductory node of the link to a set of neighbouring nodes that converse over the broken link with the destination. This recursive process obliterates all broken link entries from the routing table at each node. Since nodes reply to the first arriving RREQ packet, AODV protocol favours the least congested route instead of the shortest route. Note that the fact that the on-demand approach of the AODV protocol minimizes routing table information. AODV uses traditional routing tables as it is a reactive routing protocol. To determine whether routing information is up-to-date and to prevent routing loops sequence numbers are used. The maintenance of time-based states is a crucial feature of AODV which suggests that a routing entry that isn't recently used is expired. In case of route breakage, the neighbours are notified. The discovery of the route from source to destination relies on query and reply cycles and intermediate nodes store the route information within the type of route table entries along the route.

IV. BLACKHOLE ATTACK

The Blackhole attack is without doubt one of the recognized protection threats in ad hoc networks. The intruders utilize the black hole to carry out their malicious behaviors. Many researchers have performed different detection procedures to endorse different forms of detection schemes. Trust relationship between the nodes play an enormous function in isolating the malfunctioning nodes that roots a Blackhole attack in the community. A malfunctioning node, the so known as black gap node, could consistently reply positively to route requests even when it does not have right routing. Another case is that the Blackhole node can drop all packets forwarded to it. In other phrases, Blackhole attack is one of the assaults that publicize it for having the shortest course to destination node and drops the entire packet that is coming from source node. An illustration is provided using the Fig 1.

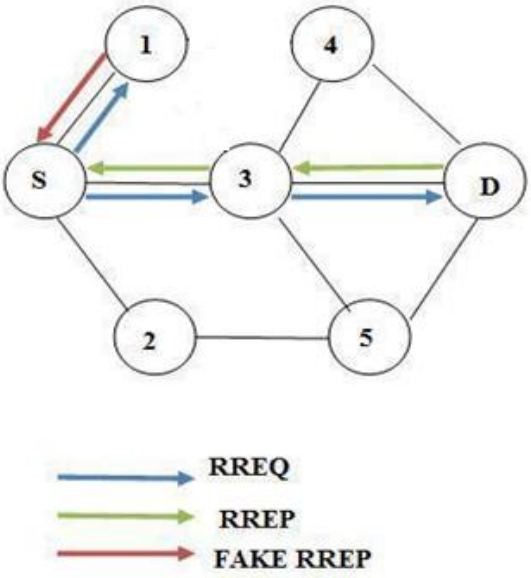


Fig. 1. Blackhole node

Node S stands for the source node and node D represents the destination node. Node 1 is a misbehavior node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest path to the destination node. For that reason, node S erroneously judges the route discovery procedure and begins to send information packets to node D. As what mentioned above, a malicious node typically drops or consumes the packets. This suspicious node will also be regarded as a black hole in MANET environment.

Single Black hole attack: In this assault, one Blackhole node drops the routing packets which it's speculated to ahead to its neighbours and claims itself of being shortest direction to destination node by means of the routing protocol.

Cooperative Blackhole attack: Blackhole is a malfunctioning node that incorrectly replies the route requests that it has a recent path to destination after which it drops all receiving packets that is to be forwarded. A threat of severe damage happens if malfunctioning nodes work collectively as a bunch. This is known as cooperative black hole attack. The intention of the Blackhole node could also be to disturb the path finding procedure or interpret the packet being dispatched to destination. For example, in AODV, the attacker can ship a fake RREP (including a false destination sequence range that's fabricated to be equal or better than the one contained inside the RREQ) to the source node, claiming that it has a sufficiently recent direction to the destination node. This causes the provide node to decide upon the route that passes via the attacker, the attacker can misuse or discard the visitors.

V. PROPOSED METHODLOGY

In this paper, we proffered a system which uses confirmation Route Request(CREQ) and confirmation Route Reply(CREP) signals for finding the presence of Blackhole in the path. If Blackhole is present in the path

means, then RREP and CREP will not be equal and we can select the next shortest path for message transfer.

A. *Network Simulation*

Simulation is regulated using NS2 2.35. Because of the link stability and route lifetime, no route overhead was considered in our simulation. In 500X500 area mobile nodes exist. Square area is used to increase average hop length of a route with relatively small nodes. Every mobile node is moving based on the mobility data files that were generated by mobility generator module. A number of 100 nodes are created. The transmission range is fixed at 100 meters. 100 nodes have destinations and try finding routes to their destination nodes. Maximum speed of node is set to 20m/sec. The nodes are assigned with an initial position. All nodes do not stop moving and the simulation time is 500 seconds.

TABLE I. SIMULATION PARAMETERS

Parameter	Value
Coverage area	500x500
Simulation Time	600ms
No of nodes	100
Traffic Type	UDP-CBR
Packet Size	512 Bytes
Maximum Speed	20 m/s
Routing Protocol	MAODV
Mobility model	Random way point
Antenna Type	Omni antenna

B.Counter attack Algorithm

The vital reason for the attacks in MANET is that the existing protocol for routing does not admit any confirmation for the Route discovered. Hence it is significant to procure a confirmation mechanism for the route established in the routing protocol. This mechanism should be efficient enough to isolate the Blackhole attack in the network. It is exhausted by introducing a distinct mode of message in existing protocol called Route Confirmation Request (CREQ) and Route Confirmation Reply (CREP). These messages assist to keep away from Blackhole attack.

C.Steps in CA Algorithm

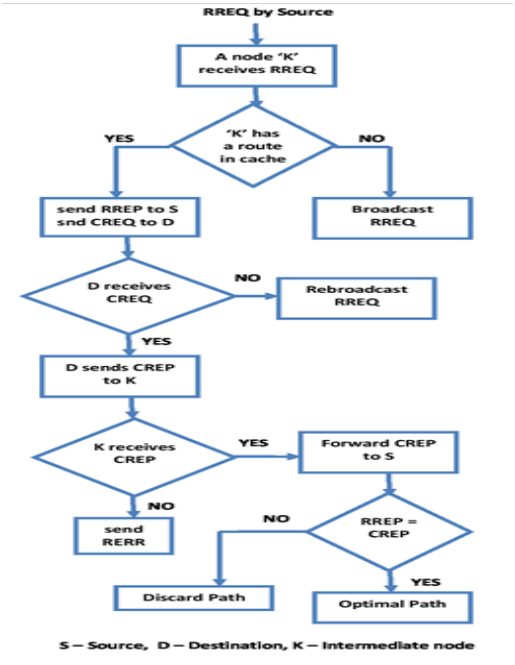
1. The Route Request (RREQ) is broadcasted to all its neighbors by the source node to discover a path to the destination.
2. As destination receives RREQ it generates a RREP message and sends to Source node to acknowledge the path established.
3. Once the Destination node sends a RREP to source node furthermore it also sends a CREQ (Confirmation Request) to its next bouncing node. If the next bounce node has a path to the source, then it generates a CREP and forward it to the source node.
4. Finally, CREP reaches the source node following the RREP. After accepting the CREP, the source node can affirm the authority of the way by contrasting the way in RREP and the one in CREP. If both are matched, the source nodes judges that the path is optimal and starts sending the packets. This method keeps the misbehaving nodes away from the routing process as they cannot insist the normal nodes to generate a false CREP packet.

This technique is more effective for attack with one Blackhole node participate in the routing process and it cannot insist its neighbors to produce a false CREP to confirm the path established. Hence this method does not involve any misbehaving nodes in the routing process. However, this protocol cannot overcome this issue when the Blackhole nodes act as a group so called Cooperative Blackhole attack. This is because when two consecutive nodes are Blackhole they can

generate false CREQ and CREP as well. Hence, this method is not incorporated for cooperative Blackhole attack.

```
Input: S-Source, D-Destination, K-Intermediate nodes.
RREQ-Route Request , RREP-Route Reply, RERR-Route Error.
CREQ-Confirmation Route Request, CREP-Confirmation Route
Reply.
1. S initiates route discovery by generating RREQ.
2. If K receives RREQ then
3.   If K has route in its cache then
4.       K generates RREP to S.
5.       K generates CREQ to D.
6.   Else Broadcast RREQ
7.   End If.
8. Else generates RERR.
9. End If.
10. If D receives CREQ then
11. D generates CREP to K.
12.  If K receives CREP then
13.  K forwarded CREP to S.
14.  Else K generates RERR to D.
15.  End If.
16. Else Rebroadcast RREQ.
17. End If.
18. If CREP==RREP then
19.    Select the path as optimal
20. Else discard the path
```

Fig. 2. CA Algorithm



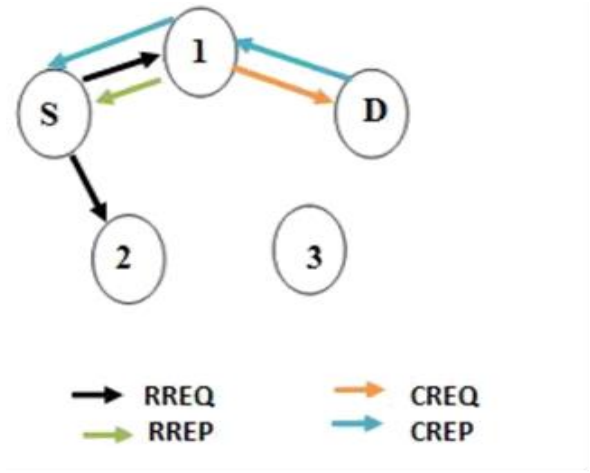


Fig. 3. Flowchart

Fig. 4. Performance of CA Algorithm

VI. Perfomance Analysis

Packet drop Ratio is evaluated with the parameters such as number of packets sent and number of packets dropped. Packet drop ratio is the ratio of number of packets dropped to the number of packets sent. It is inferred from the graph that packet drop ratio is greatly decreased in MAODV when compared to AODV and DSR. So that the quality of the message received will be increased in MAODV. From the performance analysis graph based on throughput it is observed that throughput increases in MAODV when compared to AODV and DSR.

```
void malTimer::handle(Event*)}
agent->check_mal();
scheduler::instance().schedule(this,&intr,0.5);
}
Void DSR::check_mal() {
if(index==0){
if(fcount>rcount+1) {
fprintf(stderr,"No.of packets dropped are%\n",fcount-rcount);
}
}
}
```

Fig. 5. Estimate Packet Drop during Runtime

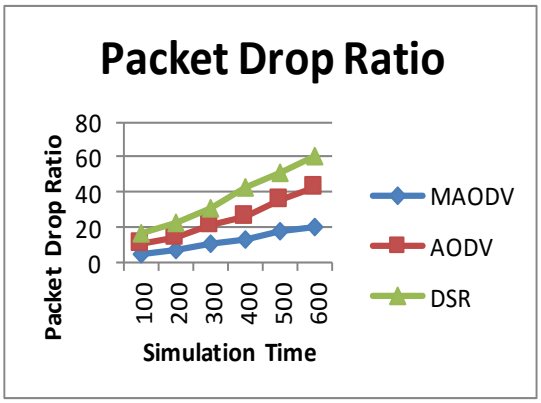


Fig. 6. Comparison of packet drop ratio between DSR, AODV and MAODV.

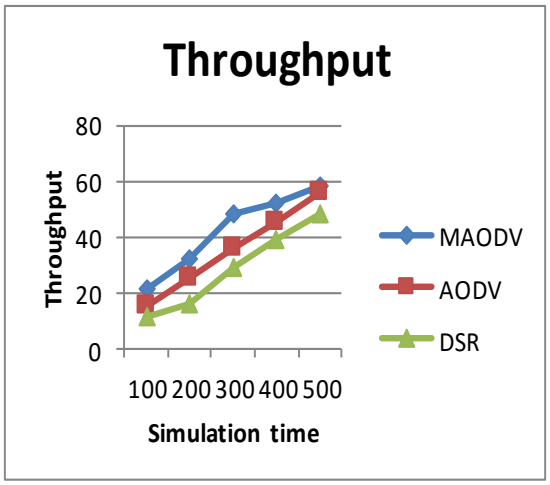


Fig. 7. Comparison of throughput between DSR, AODV and MAODV

VII. Conclusion

MANET is widely used in military and in case of natural calamities. In such circumstances the reliability of the message is very important. Blackhole node causes a great impact in the transfer of messages. By using the proffered system, the Blackhole node can be identified and we can use some other path isolating the Blackhole node so that the message reaches correctly. we have used a very simple and effective way of providing security in AODV against Blackhole attack. As the result the reliability gets increased because Blackhole node can be isolated. Our future work is to enhance this CA algorithm and use this for various attacks in MANET.

References

[1] Jhaveri, Rutvij H., Sankita J. Patel and Devesh C. Jinwala. A novel approach for grayhole and blackhole attacks in mobile ad hoc networks, *Second International Conference on Advanced Computing & Communication Technologies* IEEE (2012).

[2] Chavda, Ketan S. and Ashish V. Nimavat. Removal of black hole attack in AODV routing protocol of MANET. *Computing, Communications and Networking Technologies (ICCCNT), Fourth International Conference on* IEEE, 2013.

[3] Nisha, Simranjeet Kaur and Sandeep Arora, Analysis of Black Hole and Gray Hole Attack on RP-AODV in MANET. *International Journal of Engineering Research and Technology* 2(8): 192 - 196 (2013).

[4] Liu, Kejun, et al., An acknowledgment-based approach for the detection of routing misbehavior in MANETs. *IEEE transactions on Mobile Computing* 6(5): 536-550 (2007).

[5] Khanna, Nitin and Priyanka Sharma, Mitigating Blackhole and Grayhole Attack in MANET using Enhanced AODV with TLTB Mechanism. *International Journal of Future Generation Communication and Networking* 9(8): 129-140 (2016).

[6] Surana, K. A. and Snehal Mehatre, Securing black hole attack in routing protocol AODV in MANET

with watchdog mechanisms. *World Research Journal of Computer Architecture* 1(1): 19-23 (2012).

[7] Jain, Shalini, Mohit Jain, and Himanshu Kandwal, Advanced algorithm for detection and prevention of cooperative Black and Gray hole attacks in mobile ad hoc networks. *International Journal of Computer Applications* 1(7): 37-42 (2010).

[8] Ullah, Irshad, and Shoaib Ur Rehman, Analysis of Black Hole attack on MANETs Using different MANET routing protocols (2010).

[9] Ramaswamy, Sanjay, et al., Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks. *International conference on wireless networks* (2003).