International Journal of Advanced Technology in Engineering and Science
Vol. No.5, Issue No. 07, July 2017
www.ijates.com
ijates
ISSN 2348 - 7550

Black Hole Detection for Mobile Ad-Hoc Networks

Gourav Ahuja[1], Mrs. Sugandha[2]

[1]*Department of Computer Science and Engineering, VCE, Rohtak, Haryana (India)*

[2]*Department of Computer Science and Engineering, Asst. Prof. VCE, Rohtak, Haryana (India)*

ABSTRACT

Mobile Ad Hoc Network (MANET) is a major next generation wireless technology which is mostly used in future. MANET is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and predefine organization of available links. In a MANET mobile node will be expandable and transferable, so that attacker will be attack by a malicious node which brings great challenges to the security of Mobile Ad Hoc network. The Black hole attack is one of such security issue in MANET. Our focus is specifically is on ensuring the security against the Black hole attack with the help of the popular routing protocol which is mostly used in MANET. Mobile Ad hoc Networks (MANET) are the extension of the wireless networks. They plays important role in real life applications such as military applications, home applications etc. these networks are exposed by a lot of security attacks such as alteration, Denial of service attack, Fabrication attack etc. Black hole attack is one of the dangerous active attacks on the MANET. In this research paper an well-organized access for the detection and removal of the Black hole attack in the Mobile Ad Hoc Networks (MANET) is described. The algorithm is implemented on AODV (Ad hoc on demand Distance Vector) Routing protocol. The algorithm can detects both the single Black hole attack and the Cooperative Black hole attack.

Keywords: AODV,BLACK HOLE ATTACK,MANET,NS-3,RREP.

I.INTRODUCTION

Mobile ad-hoc networks (MANET) are formed by a group of mobile nodes, and every node in MANET can both act as host or router, and this wireless host communicate with each other without the existing of fixed infrastructure and without a central control. MANET can have more flexible because node can move any direction inside the network and it can be turn up and turndown in a very short time. In MANET there is no any base station, these mobile nodes are interconnected via wireless link which agree to cooperate and forward packet each other's. These mobile nodes in mobile Ad-Hoc network dynamically creates routes among themselves and form their own wireless network on the fly. The outmost nodes are not inside transmitter range of each other. Figure 1 shows a simple Ad-Hoc network model.

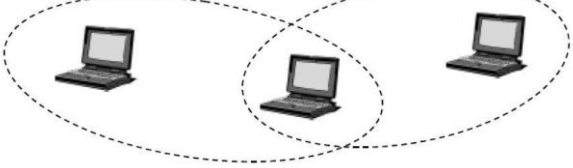


Fig. 1 Example of Simple Ad-hoc network with three participating nodes.

Routing plays an important role in the security of the entire network. Thus operations in MANETs introduce some new security problems in addition to the ones already present in fixed networks. Also the concept of trust is introduced into computing network to measure an expectation or uncertainty that an required action against attack as it has about another‘s future action. Thus, Trust can be derived from direct interactions or from recommendations. In This Paper we analyze the behaviour of black hole attack effect and provide trusted mechanism using AODV-IDS against black hole attack effect and simulation of it is done. In AODV the source node requires to send a message to some receiver node and it did not have a applicable route to the receiver, the source node initiates a path finding process for allocating all other node in the network. It then broadcasts a route request (RREQ) packet to the nodes in its close proximity, later transmitted further to their nearby nodes. This process continues to the extent up to which the receiver or an intermediate node with a "fresh" path to the target is located. When the RREQ message packet either reaches the destination node or encounters a node with a route to the destination a response is entrusted. That response occurs via the transmission of a route reply (RREP) message. In case if a node understand that the route is spoiled or sunk it transmits a route error (RERR) message to the source.

Some typical types of active attacks that can usually be easily performed against MANETs are listed as follows:

1) Black hole: A malicious node may use the routing protocol to advertise itself as having the shortest path to the node that’s whose packets it wants to intercept.

2) Denial of Service (DoS): A malicious node may generate frequent unnecessary routing requests to make the network resources unavailable to other nodes. DoS attack results when the network bandwidth is hijacked by a malicious node.

3) Impersonation: A malicious node may impersonate another node while sending the control packets to create an anomaly update in the Routing Table (RT).

4) Disclosure: A malicious node may leak confidential information to unauthorized users in the network, such as routing or location information. In the end, the attacker knows which nodes are situated on the target routing.

5) Spoofing: Spoofing occurs when a node misrepresents its identity in the network, such as by altering its MAC or IP address in outgoing packets. Spoofing combined with packet modification is really a dangerous attack.

6) Sleep deprivation: Battery powered devices in MANETs try to conserve energy by transmitting only when absolutely necessary. An attacker may attempt to consume batteries by requesting routings, or by forwarding unnecessary packets to the nodes.

II. BLACKHOLE ATTACK

A. AODV Routing Protocol

AODV [2] is an on-demand routing protocol in MANETs. Route discovery is not started until it is required (on demand).The protocol operates in two mechanisms: route discovery and route maintenance. Route discovery is used when the packet sender has no route available in its RT. It broadcasts a Route Request packet into the network. Anode receives a fresh Route Request will check its RT to see whether it has a route to the requested destination. It replies if there is one otherwise, the Route Request is forwarded. Before forwarding, it keeps a reverse path to the source node in its RT. The RT records the route information of the next hop, the distance and the current highest sequence number it has seen. Route maintenance starts when changes in the network topology invalidate a cached route. It is used to notify the source node or to trigger a new route discovery.

B. Weakness of Aodv

It is possible to exploit a number of weaknesses in AODV to disrupt the communication between nodes. We list some weaknesses of AODV as follows [3]:

1) Rush attack with RREQ: The purpose of this rush attack is to suppress a valid RREQ (request) sent by a real originator.

2) False message propagation with RREQ: The goal of this attack is to reroute traffic through the malicious node, and then throw it away.

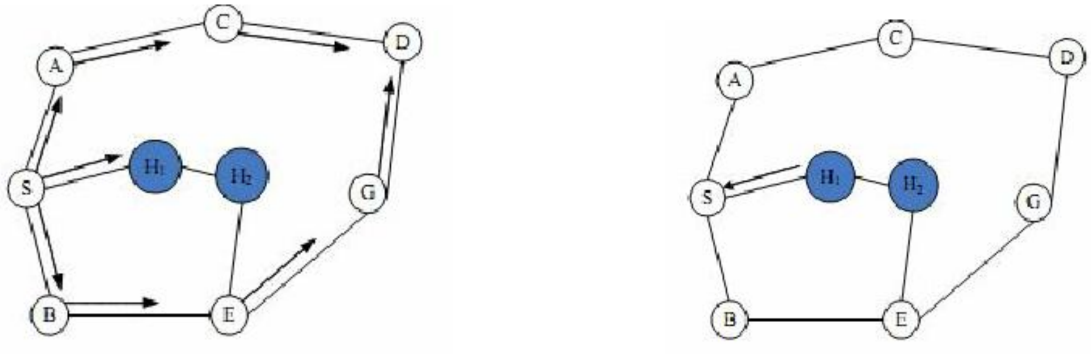
3) False reply with RREP: This attack intercepts a request with an answer, hopefully before it reaches the final destination.

4) False message propagation with RREP: In this attack the

Malicious node reroutes traffic by using false RREP packets. Again, the purpose is to create a blackhole and discard traffic.

C. Black Hole Attack

When a source node wants to send data packets to a destination node, if there has no route available in its RT ,it will initiate the routing discovery process [8], [10]. We assume node B to be a malicious node (See Figure 1). Using the routing AODV protocol, node B claims that it has the routing to the destination node whenever it receives RREQ packets, and sends the response to source node at once. The destination node may also give a reply. If the reply from a normal destination node reaches the source node of RREQ first, everything works well; but the reply from node B could reach the source node first, if node B is nearer to the source node. Moreover, node B does not need to check its RT when sending a false message; its response is more likely to reach the source node firstly. This makes the source node thinks that the routing discovery process is completed, ignores all other reply messages, and begins to send data packets. The forged routing has been created. As a result, all the packets through node B are simply consumed or lost. Node B could be said to form a black hole in the network, and we call it as the black hole attack.



(a) Network Flooding of RREQ

(b) Propagation of RREP message

III. PROPOSED METHDOLOGY

The proposed work is defined to improve the network communication and throughput in case of existence of blackhole attack in the network. The blackhole node occurs on the intermediate node on the communication path. This attacker node captures the communication data and avoids the data forwarding. Because of this, the communication loss and communication delay is increased. In more critical form, the blackhole node acts for the specific time and later on it work as the normal node. Because of this, the particular instance specific observation cannot be taken to identify the attack criticality. The proposed work model is defined to identify the black hole node in the mobile network and to generate the safe communication. The proposed has applied the dual analysis on the network nodes to identify the node criticality. The current session and the aggregative session analysis is performed based on the communication parameters. The communication throughput, loss and the communication frequency are analyzed to identify the black hole node. The nodes which accept the data for multiple sessions but not forwarded to the next session are identified. Based on this evaluation, the effective neighbor nodes are identified. The communication is performed only on the trustful reliable nodes. The method is defined to provide the effective communication against the blackhole attack.

```
/*Algorithm*/
{
1. Define Source Node S and Destination Node D
2. Set Current Node C=S
[Set C as the current node]
3. While (C<>D)
[The route formation is performed till the destination to identified]
{
    4. Nei=GenerateNeighbors(C)
    [Generate the neighbor nodes to the current nodes]
    5. For i=1 to Nei.Count
    [Process the neighbor nodes to the current node]
    {
        6. SessionComm=AnalyzeSession(Nei(i))
        [Perform the session specific communication analysis on each neighbor mobile node]
        7. AggComm=AnalyzeAggregative(Nei(i))
        [Perform the aggregative Communication over the multiple session]
        8. Node=GetEffective(SessionComm, AggComm)
[Get the effective neighbor based on the session adaptive and the aggregative communication]

9.  Set C=Node

Path.Add(C)

[Set Identified Effective Node as current node]

}

10. }

Return Path

11. }
```

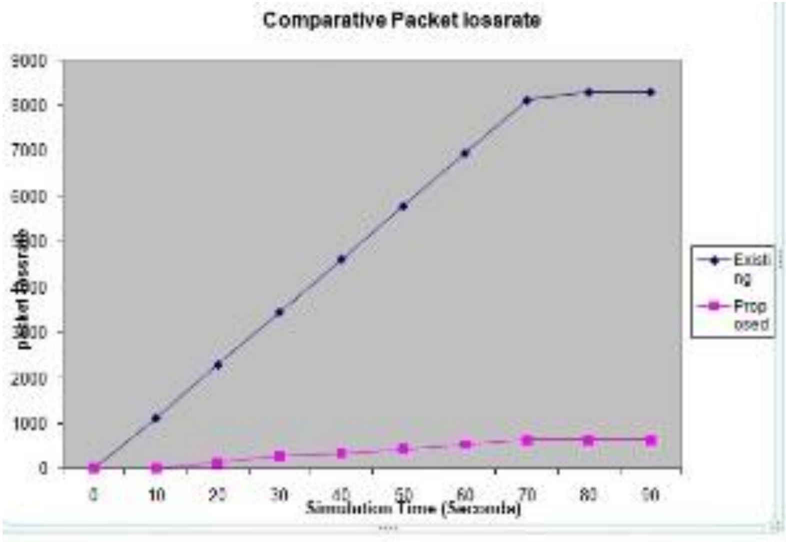


Figure 4.7 : Comparative Packet Loss Rate Analysis

IV. SIMULATION WORKFLOW

The general process of creating a simulation can be divided into several steps:

Topology definition: To ease the creation of basic facilities and define their interrelationships, ns-3 has a system of containers and helpers that facilitates this process.

Model development: Models are added to simulation (for example, UDP, IPv4, point-to-point devices and links, applications); most of the time this is done using helpers.

Node and link configuration: models set their default values (for example, the size of packets sent by an application or MTU of a point-to-point link); most of the time this is done using the attribute system.

Execution: Simulation facilities generate events, data requested by the user is logged.

Performance analysis: After the simulation is finished and data is available as a time-stamped event trace. This data can then be statistically analyzed with tools like R to draw conclusions.

V. CONCLUSION

In MANET, security is major challenges for detection and prevention the malicious node for attacker. So here we can see that attacker will be attack through a some malicious node and this attack has comes under a black hole attack and this malicious node send a fake RREP packet with higher sequence number and Absorb all the data packet. So we can detect and prevent this blackhole in some various techniques such as route discovery process, cross checking and DRI and some other way. This can be possible with the help of AODV routing protocol. Detection and prevention arises some defect which is packet delivery is low and consume a more time. So we solve these issues with the help of timer based and RRCT to SAODV to delivery packet with correct route.

VI. FUTURE WORK

Future work is focused on design an algorithm for minimum delay and reduce packet dropping ratio and increase more packet delivery ratio in case of mobility of nodes in mobile Ad-hoc network. And also try to enhance the efficiency of mobile Ad-hoc network.

REFERENCES

[1] Prachi Goyal & Chitvan Gupta, NIET "An Approach for Security Measures of Black Hole Attack in MANET" , International Journal of Emerging Trends in Science and Technology, IJETST-Vol.03,January, 2016.

[2] Harshil B.Jani & Hardik Prajapati, "Detection of black hole attack in manet",international journal of current engineering and scientific research, volume-3, issue-4, 2016 .

[3] Junhai Luo & Mingyu Fan," Black Hole Attack Prevention Based Authentication Mechanism", 1-4244-2424- 5/08/2008 IEEE.

[4] Chinky Jain& Pardeep Tyagi, "Simulation of Black Hole Attack in Manet", International Journal Of Engg. And Computer Science ISSN: 2319-7242 Volume 5 Issue 08 August 2016.

[5] Nigahat & Dr. Dinesh Kumar, "a review of black hole attack n mobile ad hoc networks, international journal of engineering science research technology, issn :2277- 9655, march 2017.

[6] T.Manikandan, S.Shitharth, C.Senthilkumar, "Removal of Selective Black Hole Attack in MANET by AODV Protocol", International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Special Issue 3, March 2014.

[7] Kavi Joshi, Er.Manoj Kumar, "Three Way Techniques for Preventing BlackHole Attack in MANET Using AODV Protocol", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 2, February 2016.

[8] Ei Ei Khin1 and Thandar Phyu, "impact of black hole attack on aodv routing", Inter- national Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.2, May 2014.

[9] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", Human-centric Computing and Information Sciences 2011.

[10] Rajib Das**, "**Security Measures for Black Hole Attack in manet: An Approach",International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Special Issue 3, March 2012.

[11] Ajesha Patel & Anurag Jain "A study of various Black Hole Attack techniques and IDS in MANET", International Journal of Advanced Computer Technology (IJACT), volume 4, number 3,2015.

[12] Nakka Nandini, Reena Aggarwal, "Prevention of black hole attack by different methods in MANET" International Journal of Advanced Research in Computer Engineering Technology (IJARCET) Volume 4 Issue 2,February 2015.

.