Volume 4, Issue 8, August 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Detection and Prevention of Black Hole Attack with Digital Signature

Ravinder Kaur
M.tech Scholar(CSE), GNIT, Ambala
Kurukshetra, Haryana, India

Jyoti Kalra
Asst. Prof., GNIT, Ambala
Kurukshetra, Haryana, India

***Abstract**: A mobile ad hoc network (MANET) is infrastructures less dynamic network consist of a collection of wireless mobile nodes that communicate with each other without the use of any centralized network. Security in MANET is the most important concern for the basic functionality of network. The dynamic topology of MANETs allows nodes to join and leave network at any point. Security of AODV protocol is compromised. By a particular type of attack called black hole attack. A malicious node advertises itself as having the shortest path to the node whose packets it want to intercept. In this paper we are trying to find the secure path for transmission through Digital Signature. Digital Signature is the verification technique.*

***Keyword:** MANET, AODV, Black Hole Attack, Single Black Hole Attack, Cooperative Black Hole Attack, Digital Signature.*

I. INTRODUCTION

In a MANET, a collection of mobile hosts with wireless network interfaces form a temporary network without the aid of any fixed infrastructure or centralized .Due to absence of any kind fixed infrastructure and open wireless medium security implementation is difficult. In MANET each node functions as a host as well as router, forwarding packets for another node in the network. MANET is vulnerable to various kinds of attacks. These include active route interfering, imprecation and denial of service. Black hole attack is one of many possible attacks in MANET. In this attack, a malicious node sends a forged Route REPLY (RREP) packet to a source node that initiates the route discovery in order to pretend to be a destination node. The malicious node launches this attack by advertising fresh route with least hop count and highest destination sequence number to the node which starts the route discovery.

Fig 1: Route discovery process

II. AODV ROUTING PROTOCOL

AODV is an on demand distance vector routing protocol. In on demand routing a route is established between communicating nodes only. There is no fixed existing route as in table driven systems. Whenever a node needs to send data packets it has to initiate route discovery process. Route discovery consists of two messages: Route Request (RREQ) and Route Reply (RREP).

The source node broadcasts the RREQ messages to its neighbors which further broadcasts them to their neighbors and so on. In response to RREQ, either the destination node replies with RREP or intermediate node having route to destination replies with RREP.

When intermediate node replies it is called Gratuitous Route Reply. Validity and freshness of route is decided by destination sequence number. If destination sequence number is higher than before than route is considered valid. Source selects the path for data packets transmission from which it received RREP first. Further received RREPs are discarded.

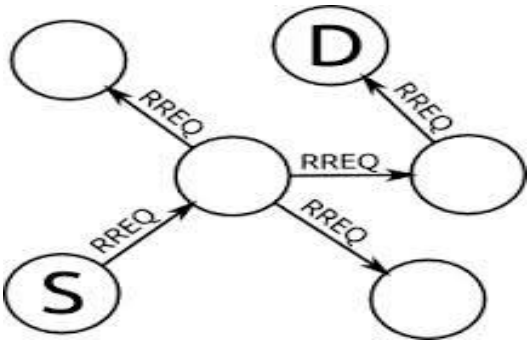

Fig 2: AODV routing protocol with RREQ

With RREQ and RREP message [12]. For route maintenance nodes periodically send HELLO messages to neighbor nodes. If a node fails to receive three consecutive HELLO messages from a neighbor, it concludes that link to that specific node is down. A node that detects a broken link sends a Route Error (RERR) message to any upstream node.

III. BLACKHOLE ATTACK

Black hole problem in MANETS [2] is a serious security problem to be solved. In this problem, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept.

A. Single Black Hole Attack

AODV route discovery mechanism is based on RREQ/RREP messages. Source node broadcasts the RREQ message to its neighbors. Either the destination or intermediate node sends RREP. The RREP received first by source node is accepted and all further RREPs are discarded. Black hole node takes benefit of this feature of AODV and sends RREP first even without checking its routing table. In this way, a route through black hole node is setup and black hole node consumes all the forwarded packets

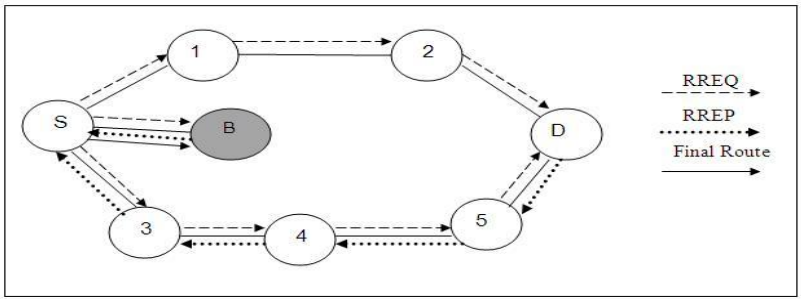

Fig 4: Single Black Hole Attack

In figure 4, B is black hole node through which final route is established. Being the black hole node, it consumes all the packets without forwarding them.

B. Cooperative Black Hole Attack

Cooperative Black hole means the malicious nodes act in a group [10][11]. As an example, consider the following scenario in figure 5.

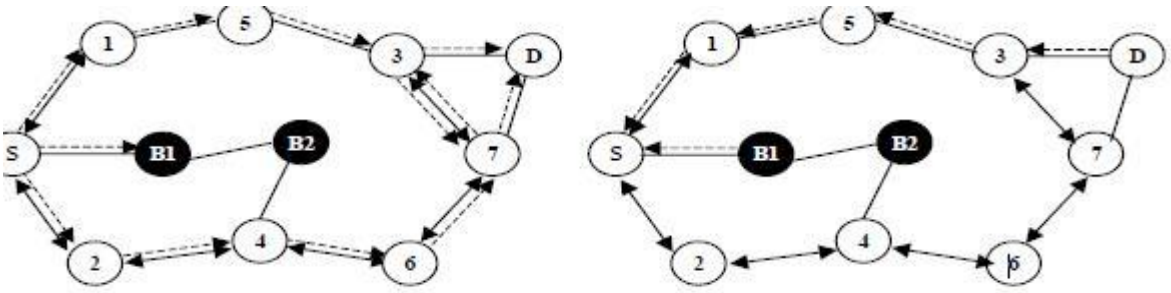

Fig 5: cooperative black hole attack

In above Example, when multiple black hole nodes are acting in coordination with each other, the first black hole node B1 refers to one of its teammates B2 as the next hop, as depicted .In Figure 5. According to [13], the source node S sends a "Further Request (FRq)" to B2 through a different route (S-2-4-B2) other than via B1. Node S asks B2 if it has a route to node B1 and a route to destination node D. Because B2 is cooperating with B1, its "Further Reply (FRp)" will be "yes" to both the questions, then all the packets are consumed by node B1 and the security of the network is compromised.

IV. PROBLEM STATEMENT

Cooperative Black hole attack is the one of the serious problem in MANET. Mobility is the main issue to security. Path is created on demand whenever needed. Malicious nodes become barrior in the secure path. It drops the entire packet and stops them to reach at the destination. Detect the malicious node and created the shortest path is the problem that is going to solve.

V. PROPOSED SOLUTION

In this dissertation, to detect the malicious node in network digital signatures are used. Digital signature is the one of the verification technique. All nodes have legitimate digital signature. In AODV the route request is send to neighbor nodes by the source node. If destination node is one of them then ok otherwise route request broadcast to next node until the destination is found. The route request (RREQ) packet header contains the information of visiting node (node-id) in node information column and hop count column which contains the number of visiting nodes used in path. At the destination TTL scheme is used. the destination node select the shortest path with minimum number of nodes. the destination node unicast the reply whose header contain the column of node-id that contains the id of all nodes used in that path and digital signature column in which each visiting node adds its digital signature. When the receiving node received packet compare the digital signature of the previous node from its database. if the signature is match then that node is legitimate otherwise that node is considered as malicious node. When malicious node is detected then that info is broadcast to the neighbors. This process is repeated until the secure path is not found.

Algorithm:

Algo(Blackhole_attack_detection)
Input: no. of nodes n, Source node, Destination Node;
Output: Detection and prevention of Black hole Attack, Find the Best Path for routing;
Begin
Create the network for the input node(of n number nodes)
Define Source node & Destination Node
Find the neighbors node of source node
For source to destination
Send Route Request to neighbor nodes for finding the destination
If next node is destination
Then direct path is established
Else
Broadcast the RREQ to next neighbors
End for
For destination to source
Select the path with average hop counts
Unicast RREP to pervious node with digital signature
Verify digital signature
If (all signatures are legal)
Establish a path for data transfer.
If (Any intermediate or destination node is malicious node)
Then add the malicious node information in malicious node column and again rebroadcast Route request (RREQ)
End for
End

VI. SIMULATION AND RESULT

The model is simulated in MATLAB 7.10.0.499. The presented model can be used for large Mobile ad hoc network. Initially there is a network in which nodes are distributed randomly as shown in Figure

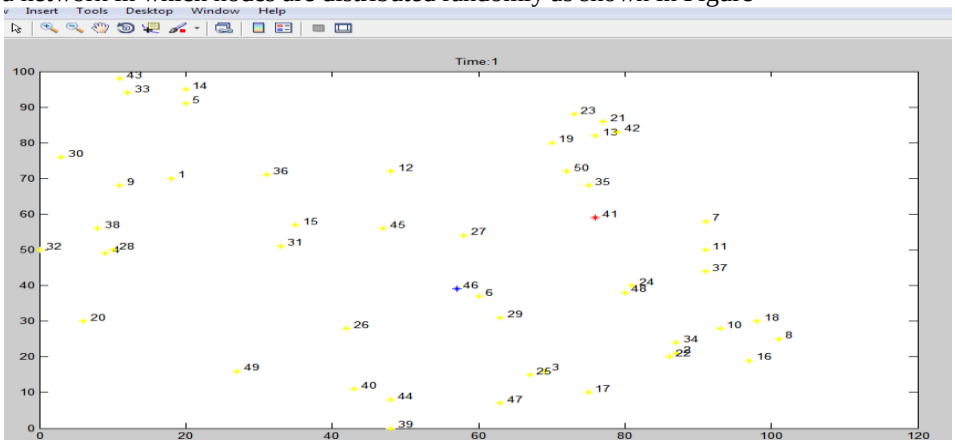

Fig 7: Network creation using 50 Nodes.

The figure 7 shows the node 50 is source node and node 27 is the destinations node. The node 50 broadcast the route request with in communication range. The node 35 and 19 receive the RREQ packet and forward to the next node. This process is going on when the packet reaches the destination node.

Figure 8 shows the best path find out while run the simulation. In this simulation the 41 node is malicious node. Here 5 rounds of simulation is performed and path is find every time. Sometime path can't be establish because of node not in range.

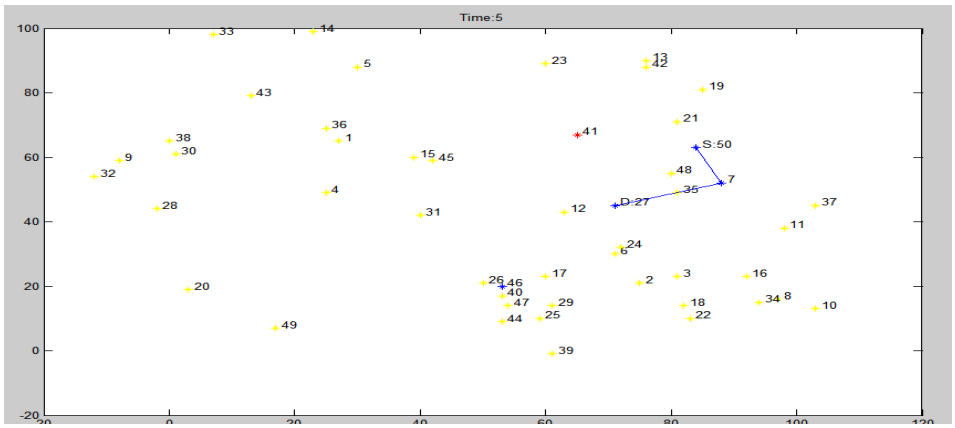

Fig 8: Path establish from source to destination

Here the source is 50 and the destination is 27. Every time a new path is found. Because of mobility nodes move from one location to another. the path that show figure is 50- 7- 27.

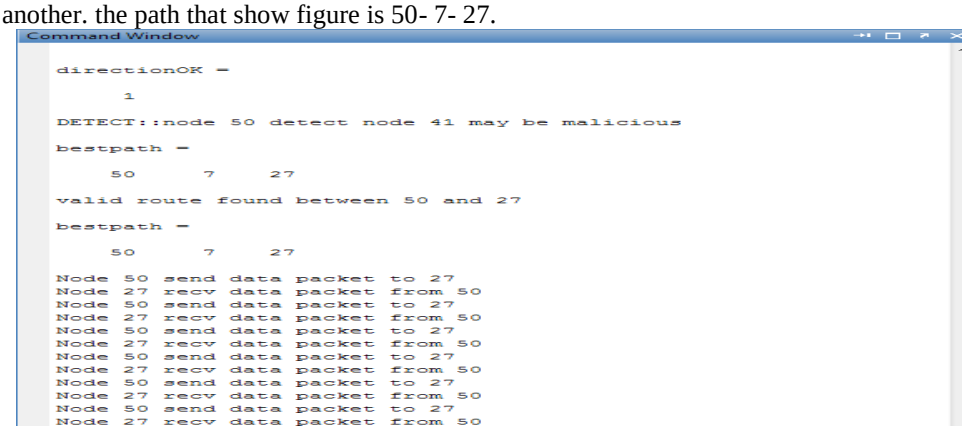

Fig 9: Detect Malicious Node

This figure shows that malicious node presnt in the network. This node is detect by source node through digital signature.when the malicious node detect by source node it sent the informaiont to all neighbor nodes. When the malicious node is detect in path that path is not select by any node.

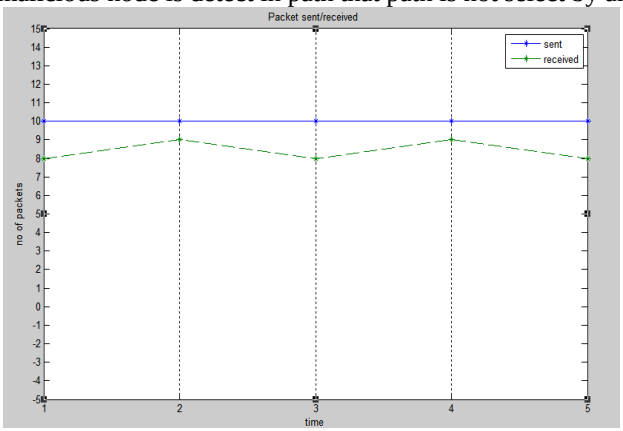

Fig 10: Using Digital Signature data Sent and Receive

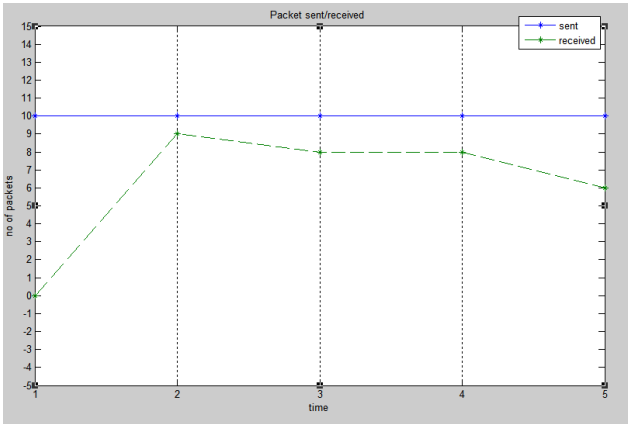

Fig 11 :Without digital signature data Sent and Receive

Figure 10 represent the graphical presentation with digital signature. The simulation runs 5 rounds. In first round malicious node exist in the path. The source node send 10 packets but at the destination node 8 packet reach because the power depletion. In second round 10 packets send, at this time black hole node did not in the path so 9 packets reached at the destination. Third round again black hole did not exist in the path and 8 packets received. In fourth round 10 packets send and 8 packets received. In fifth round 10 packets are sent but at receiving only 6 packets within communication range deplete the power. Figure 11 represent the graphical presentation without digital signature. The simulation runs 5

rounds. In first round malicious node exist in the path. The source node sends 10 packets but at the destination node no packet reach because the black hole node drops all the packets. In second round 10 packets send, at this time black hole node did not in the path so 9 packets reached at the destination. Third round again black hole did not exist in the path and 8 packets received. In fourth round 10 packets send and 8 packets received. In fifth round 10 packets are sent but at receiving only 6 packets within communication range deplete the power.

VII. CONCLUSION AND FUTURE WORK

This research providing an efficient technique in the network that detects the malicious node in the network. Mobility is the main issue in network. Due to their dynamic nature, it will require higher security. The solution is implemented on 50 nodes. the future work of this is to remove the flooding problem.

REFERENCES

[1] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard,"Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", www.cs.ndsu.nodak.edu/~nygard/research /BlackHoleMANET.pdf 2003 .

[2] "Prevention of Co-operative Black Hole Attack in MANET" Latha Tamilselvan BSA Crescent Engineering College, Vandalur, Chennai, Tamilnadu, India, Ph.: 91 44 2275 1375, Fax: 91 44 4211 4282,Email: latatamil@hotmail.com Dr. V Sankaranarayanan BSA Crescent Engineering College,Vandalur, Chennai, Tamilnadu, India, Ph.: 91 44 2275 1375, Email: sankarammu@yahoo.com

[3] Akshat Jain, Shekher singh Sengar, Vikas Goel "Colluding Black Holes Detection in MANET" International Journal of Engineering Research & Technology (IJERT) ,Vol. 2 Issue 1, January- 2013 ISSN: 2278-0181

[4] Dokurer, Semih "Simulation of Black hole attack in wireless Ad-Hoc networks" Master's thesis, Atihm University, September 2006.

[5] Latha Tamilselvan, V sankaranarayanan, "Prevention of Blackhole Attack in MANET". In Proceedings of The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007), pp. 21-21, Aug. 2007.

[6] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour and Y. Nemoto " Detecting Black hole attack on AODVbased mobile ad hoc networks by Dynamic Learning Method", Intl. Journal of Network Security, vol 5, no 3 Nov 2007, Pp 338-346.

[7] Sun, Y. Guan, J. Chen and U.W. Pooch, "Detecting black-hole attack in mobile ad hoc networks", Proc. 5th European Personal Mobile Communications Conference, Apr. 2003, pp. 490-495.

[8] E. Perkins and E. M. Royer, "The Ad Hoc On-Demand Distance Vector Protocol", Ad hoc Networking, Addison-Wesley, 2000, pp. 173-219.

[9] Elizabeth M. Royer, C-K Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks".

[10] Anu Bala, Jagpreet Singh and Munish Bansal "Performance Analysis of MANET under Blackhole Attack" First International Conference on Network and Communication 2009

[11] Bracha Hod, "Cooperative and Reliable Packet-Forwarding On Top of AODV",www.cs.huji.ac.il/~dolev/pubs/reliable-aodv.pdf, 2005 .

[12] Tamilarasan-Santhamurthy; "A Comparative Study of Multi-Hop wireless Ad-Hoc Network Routing Protocols176-184.ISSN(online):1694-0814

[13] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad HocinMANET", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3,September 2011, PP:Network," IEEE Com

[14] Dokurer .S, Y. M. Erten , Can Erkin Acar "Performance analysis of ad-hoc networks under black hole attacks",Turkey

[15] Mohammad Al-Shurman and Seong-Moo Yoon and Seungjin Park, "Black Hole Attack in Mobile Ad HocNetworks"

[16] "An Efficient Wormhole Prevention in MANET Through Digital Signature" Anil Kumar Fatehpuria1, Sandeep Raghuwanshi, International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 3, March 2013)

