Volume 4, Issue 6, June 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review Paper on Detection and Prevention of Black hole in MANET

Ravinder Kaur
M.tech,(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 authority. 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.

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 function as a host as well as router, forwarding packets for another nodes in the network. MANET is vulnerable to various kind 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.

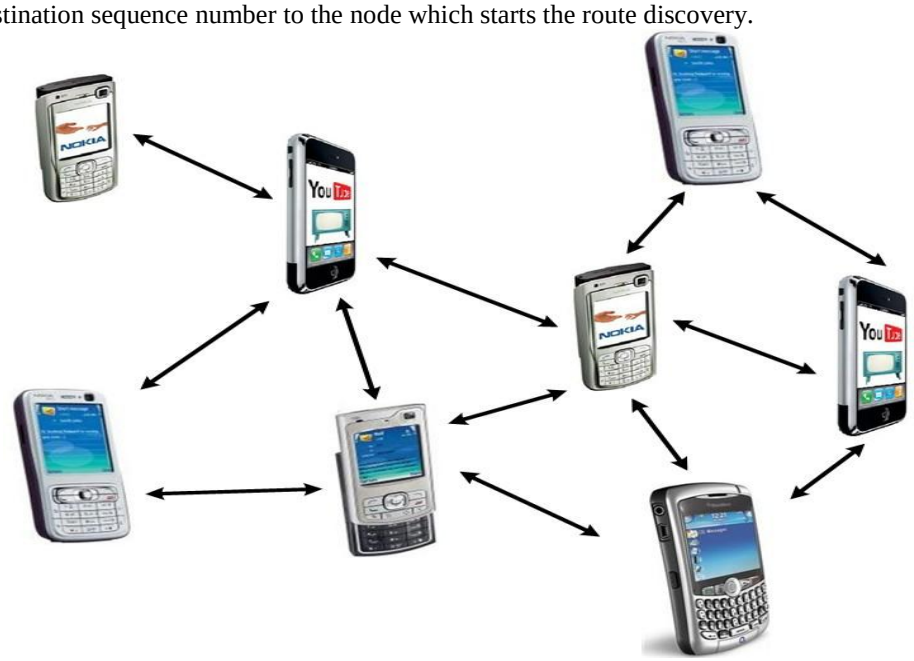

Fig 1: Route discovery process

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.

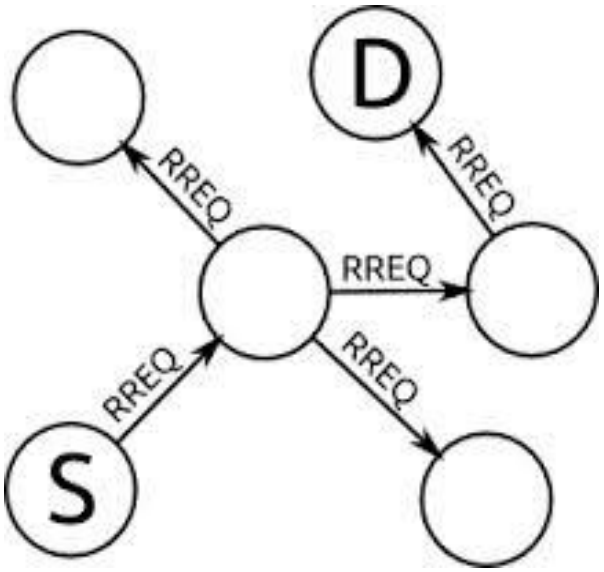

Fig: 2, AODV routing protocol with RREQ

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.

1) INTERNAL BLACKHOLE ATTACK

In this attack malicious node fits in between the routes of source and destination. As its present internally so this node make itself an active data route element. Now that node is capable of conducting attack in network. Internal attack is more sever then external attack.

2) EXTERNAL BLACK HOLE ATTACK

External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET. In this

- Malicious node detects the active route and notes the destination address.
- Then Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
- Malicious node send RREP to the nearest available node which belongs to the active route. This can be send directly to the data source node if route is available.
- The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node. The new information received in the route reply will allow the source node to update its routing table.
- New route selected by source node for selecting data. The malicious node will drop now all the data to which it belong in the route because is presented inside the network.

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

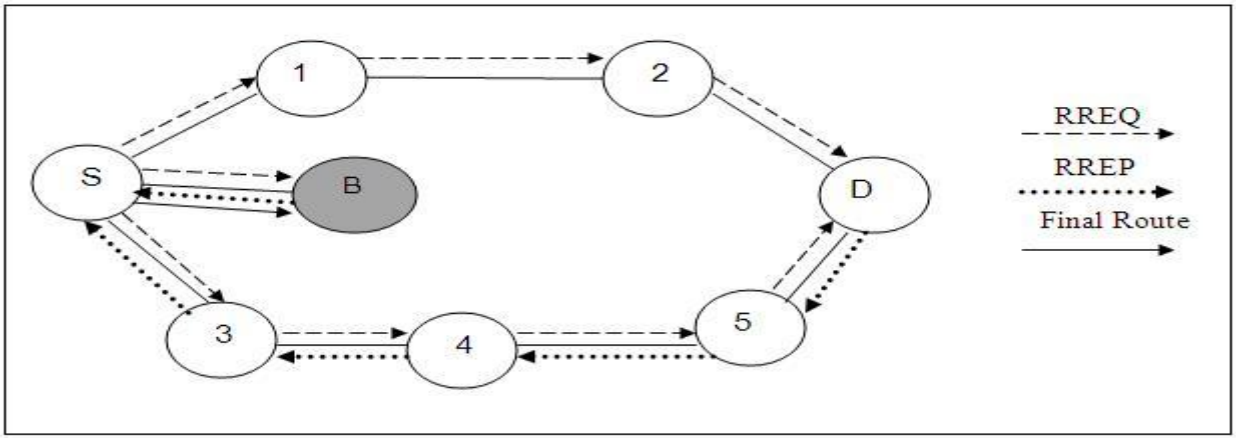

Fig. 4. Single Black Hole Attack

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.

Solutions

In [3], RREP packet is required by intermediate node to send information about next hop. On receiving this RREP packet, source node sends a Further Request to next hop to verify that it has route to intermediate node that sends the RREP packet and it has route to destination. Further Reply is sent by next node in response to Further Request.

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.

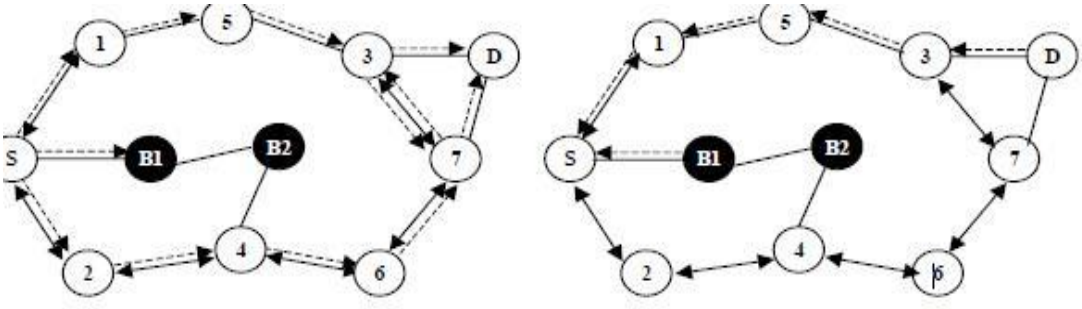

Fig 5 cooperative black hole attack

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. Now per the solution proposed in [13], node S starts passing the data packets assuming that the route S - B1-B2 is secure. However, in reality, the packets are consumed by node B1 and the security of the network is compromised.

IV. Proposal solution

This research will focus on providing an efficient technique in the network that detect the malicious node in the network. Malicious node has 2 properties: it always attack on the active route in the network and it sends the RREP first before the others. I have using the verification technique Digital signature for the solution. Every node in the network has its own digital signature. It gives the better security .

V. Conclusion and Future work

This paper mainly focused on the black hole attack in network. How it is detect from the network .How can we prevent our data from malicious node . Due to their dynamic nature, it will require higher security. A future scope of this is to find an effective solution to the black hole attack on AODV.

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).

