Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 1, January 2015, pg.415 – 420

SURVEY ARTICLE

A Survey on Black Hole Attack Detection in MANET Using AODV Protocol

Ashwini S Hosgouda[1], Prof. M.S Shobha[2]

Student, M.Tech (Software Engineering), NHCE, Bangalore, India[1]

Assistant Professor, Information Science & Engineering Department, NHCE, Bangalore, India[2]

ashwinihosgouda@gmail.com

Abstract- Mobile ad hoc networks (MANET) are dynamic, decentralized and infrastructure less network, where at any given point of time nodes can join or leave the network. Due to the property of flexibility and simplicity MANET are widely used in military communication, mobile conferencing and emergency communication. As ad hoc networks are autonomous mobile nodes, they form a temporary based network which has no fixed infrastructure. Every node in the network is autonomous hence they act as host as well as router. Due to this nature of MANET, where any node can join or leave the network without any permission, security is the main challenge in such networks. One of the major security issues in MANET is Black hole attack. It occurs when a malicious node referred as black hole joins the network. during the process of discovering route this node acts as if it has the route to the destination and takes all the packets into it and does not forward to the desired destination, Instead it drops all the packets. In this paper, we have survey on few of the techniques and methodologies for detecting and preventing black hole attack in MANET using AODV routing protocol and a table representing their flaws.

Keywords: MANET, AODV Routing Protocol, Ad hoc network, Black hole

I. INTRODUCTION

Wireless ad hoc networks are group of autonomous nodes that can be self managed with no infrastructure. MANETS are spontaneous and dynamic in nature so any node can join or leave the network at any given time. Due to this they are widely used in military and rescue areas where communication among soldiers in battlefield and in areas where new temporary network is required because the network might be collapsed due to some disaster. Ad hoc networks are temporary networks which are established in place where no fixed infrastructure is required.

The nodes act as both host and router they exchange and forward packets for their communication. MANET use routing protocols for such communication, they can be either proactive routing protocol(table driven routing protocol) in which routing information of nodes are exchanged periodically such as DSDV- destination sequenced distance vector, OLSR- optimized link state routing

protocol. Or reactive routing protocol(on-demand routing protocol) in which route is established and nodes exchange information only when needed such as AODV- ad hoc on demand distance vector, DSR- dynamic source vector.

Apart from nodes acting as host they also act as router in discovering nodes and forwarding packets to the correct node in the network. As wireless ad hoc networks have no fixed infrastructure they are more open to attacks. One of the major attacks is the black hole attack. In which the malicious node absorbs all the packets in it like a hole which sucks in everything, hence it is named as black hole attack.

In the AODV routing protocol the process of route discovering is done by the intermediate nodes which are responsible for finding fresh path to the destination by sending discovery packets to the neighbor nodes. Malicious node does not fallow this process instead it immediately responds to the source node with false information stating it has the fresh path to the destination. Source node then sends all its packets to the destination via this malicious node assuming it has the route. Black hole attack occurs when this malicious node drops all the packets and does not send packets to the desired destination node.

II. AODV ROUTING PROTOCOL

AODV is a reactive routing protocol in this network generates route to start the communication. It does not maintain any routing information or does not participate in any periodic routing table exchange. It does not have to keep track of the route information neither discover the route until the two nodes needs to communicate with each other. In the below figure, AODV route discovery process is explained.

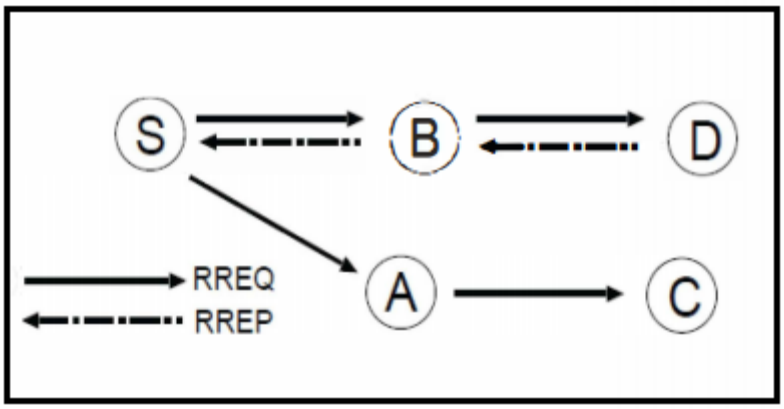

Figure1. AODV route discovery process

In the figure node S is the source node trying to establish route to the destination node D, if S does not have route information about D in its table it simply broadcast route request packets RREQ to all its neighbor nodes. When node A and B receive RREQ packet it checks in its respective routing table for the fresh route to the destination. If it has the route for destination it reply back to the source node using RREP packet and the source node send packets via the intermediate node by changing the route table information in its node.

If the intermediate node does not have a fresh path to the destination it simply broadcast the RREQ packet to its neighbor nodes and this is done until the destination node D receives RREQ packet. When node D receive RREQ packet it sends back reply using RREP packet hence a connection is established between node S and node D. In case when source node S receives multiple RREP's it selects the one with higher destination sequence number and if all the RREP's have same destination sequence number it considers the one with lower hope count value.

III. BLACK HOLE ATTACK

A black hole attack is a kind of denial of service attack in which a malicious node absorb all packets in itself by falsely claiming a fresh route to the destination and drop them without forwarding them to the destination. In this kind of attack the faulty node advertise itself for having a fresh route and shortest path to the destination without even checking its routing table information

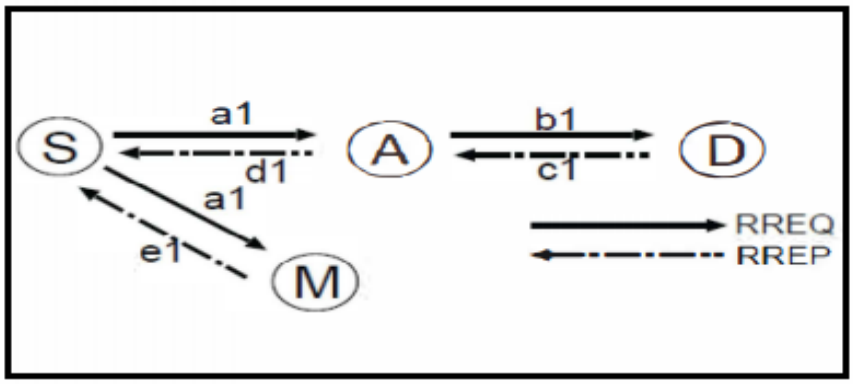

Figure2. Black hole attack

In the above figure, S is the source node which wants to send packets to D the destination node. Every node has two type of packets to be sent to the destination, one is routing packet and other is data packet. When node S wants to send data packets to node D it sends the route packets also called as (RREQ) route request packet to its neighboring nodes.

Let us assume that nose M is faulty node, after getting the RREQ packet from S it immediately reply back stating that it has fresh path to the destination without even checking its routing table. Once node S has got the (RREP) route reply packet from M it sends all data packets to M thinking it has the shortest and fresh path to the destination. But node M does not forward packets to the destination instead drops all packets. Node M reply back with minimal hope count value and highest destination sequence number so source node S sends all its packets to the malicious node M. With this attack all the data packets are falsely taken from the source node and are dropped without sending to the destination.

Two types of black hole attack

1. ***Internal black hole attack***

   Here the faulty node is present inside the network. It takes part actively in the communication of source and destination. This is called as internal attack because the malicious node belongs to the network internally. This attack is more severe as the malicious node actively takes part in the network.

2. ***External black hole attack***

   Here the faulty node stay outside the network and deny access to network traffic. This attack can become internal attack when it takes control of internal malicious node and control it to attack other nodes in the network.

IV. TECHNIQUES FOR DETECTION AND PREVENTION OF BLACK HOLE ATTACK

A. "DRl Table and Cross Checking Scheme" [1, 2] Hesiri Weerasinghe planned an algorithmic program to determine cooperative Black Hole Attack. In this a slight modification is done to the AODV routing protocol by adding an additional table i.e. Data Routing Information (DRI) table and crosschecking using Further Request - FREQ and Further Reply – FREP . DRI table helps in keeping track of whether or not the node took part in data transfers with its neighbors. Each entry within the table concerning their neighbor to indicate whether or not the node has sent data through or from that the neighbor node. If there is no route to the destination, the source node can broadcast a Route Request packet –RREQ to seek out a safe and secure path to the destination node same as in the AODV. once the intermediate node receives RREQ it will reply for the request or again broadcasts it to the network it depends on the availability of fresh route to the destination. If the destination encompasses a reply, all intermediate nodes update its routing entry for that destination. Source node additionally send data on the path because it trust the destination and updates the DRI table with all intermediate nodes between source and therefore the destination.

B. "Detection, Prevention and Reactive AODV (DPRAODV) Scheme"[3] New packet named ALARM is used in DPRAODV scheme. In this scheme an extra check is done on the threshold value. The REP sequence number is checked to examine whether its value is higher than the threshold value or not. If the value of RREP sequence number is higher than the threshold value, the node is referred as a malicious node and updated it to black list. The ALARM is sent to its neighbor nodes, each having the black list. So whenever RREQ comes from a node the intermediate nodes check if the sender node is in the black list if is, it will simply reject packets from that node. Thus the RREP from the malicious node is blocked. The advantage of DDPAODV is that it has higher packet delivery ration than the original AODV, but it takes bit higher routing overhead and end to end delay. It does not support cooperative black hole attack.

C. "Time-based Threshold Detection Scheme" [4] Tamilselvan L proposed a technique which is the enhancement of the original AODV routing protocol. The major concept is, once the first request if found collection of requests from other nodes is done by using a timer. Collect Route Reply Table (CRRT) is used for collecting the sequence numbers and the time value. By comparing the arrival time of the first request and the threshold value route request value of the network is measured. The simulation result shows that a higher packet delivery ratio is obtained with only minimal delay and overhead. Disadvantage is end-to-end delay when the malicious node is away from the source node.

D. ***"Trust Table Method" [5]*** in this method, a data structure referred as trust table is provided to every node. This table is responsible for holding the addresses of the reliable nodes. An extra field called as trust field is attached to RREP packet. This field indicates the reliability of the replying node. Only if the RREP is propagated by a reliable node the source node sends its data through it, Otherwise it waits for further RREP.

E. "Neighborhood-based and Routing Recovery Scheme" [6] in this method black hole attack is detected based on the neighbor set information. It consists of two parts: detection and response. Two major steps in detection procedure are collection of neighbor set information and finding the black hole attack. In Response procedure, Source node sends a modify-Route Entry (MRE) control packet to the Destination node to form a accurate path by modifying the routing entries of the intermediate nodes from source to destination. This scheme is more effective in detecting black hole attack with less routing control overhead to the network. The demerit of this scheme is that it becomes useless when the attacker agrees to forge the fake reply packets.

F. "Nital mistry et al's Method" [7] this method has proposed an improved security of AODV routing protocol against Black hole Attack. In this method the working of source node is modified by adding new parameter Pre_Receive_Reply. Along with this a table Cmg_RREP _Tab, a variable Mali node and a new timer MOS _WAIT_TIME are also added to the original AODV. In this method, The source node waits for MOS _WAIT_TIME after receiving the first RREP and at the same time it stores all the RREPs in the Cmg_ RREP _Tab table until MOS _WAIT_TIME. Now by analyzing the stored RREPs source node will discard the RREP with higher destination sequence number. A node is said to be malicious node referred as mail node, if the node has sent the RREP with high destination sequence number. And it also helps in discarding messages coming from that node in future. The Packet delivery ratio is increased by 81.812% in presence of black hole attack compared to AODV and there is 13.28% rise in end-to end delay.

V. COMPARISON OF DIFFERENT METHODS FOR DETECTION AND PREVENTION OF BLACK HOLE ATTACK

METHOD	ADVANTAGES	DISADVANTAGES
DRI table and cross checking schema	Supports cooperative black hole attack	Cannot support gray hole attack.
Detection, prevention and reactive AODV schema	Packet delivery ratio is increased compared to original AODV.	Increased routing overhead and end to end delay. And does not support cooperative black hole attack.
Time based threshold detection schema	Higher packet delivery ratio with minimal delay and overhead.	End to end delay is increased when the faulty node is far away from source node
Trust table method	Support the detection of multiple black hole attack.	Increased end to end delay.
Neighborhood based and routing recovery schema	15% of increased packet throughput.	It becomes useless when the attacker agrees to forge the fake reply packets.
Nital Mistry et al 'S Method	Supports black hole attack.	Cannot support cooperative black hole attack and has time delay problem.

VI. CONCLUSION AND FUTURE WORK

A Black Hole attack is one among the most important security issues in MANETs. During this a malicious node impersonates a destination node by sending false RREP to the source node and collects all the packets in itself and drops them. In AODV routing protocol the main security threat that degrades the performance is the black hole attack. Its detection is the main matter of concern. In MANET there are several disadvantages of routing protocols thus researchers have conducted numerous techniques to propose different types of detection and prevention mechanisms for black hole attack.

In this paper a survey on different existing techniques for detection of black hole attacks with their defects is presented. These methods have benefits like higher packet delivery or support multiple black hole attack at the same time. All of these methodologies have some or the opposite drawbacks, either it might be having higher overhead, higher packet loss, doesn't support cooperative black hole attack or increased end to end delay. Primarily based on the above performance comparisons, it can be concluded that Black Hole attack affects network negatively. Thus there is a desire for perfect detection and elimination of black-hole mechanism that relies on cluster organization of network. This supports cooperative black hole attack and additionally offers way to facilities the server node to overcome the failure. Thus providing security for Black hole attack and Efficient in detection and prevention are the future need for Ad hoc networks.

REFERENCES

[1] Hesiri Weerasinghe and Huirong Fu, *Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation*, Intenation Journal of Software Engineering and its Application, Vol.2, Issue 3, July 2008.

[2] Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K, *Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks*, Paper presented at the International Conference on Wireless Networks, Las Vegas, Nevada, USA, 23-26 June 2003.

[3] Raj PN, Swadas PB, *DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANEr*, International Journal of Computer Science Issue, Vol. 2, pp 54-59, 2009.

[4] Tamilselvan L, Sankaranarayanan V, *Prevention of Blackhole Attack in MANET*, 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27-30 August 2007.

[5] Yaser khamayseh, Abdulraheem Bader, Wail Mardini, Muneer BaniYasein, in "*A New Protocol for Detecting Black Hole Nodes in Adhoc Network*, Internalional Journal of COllununication Networks and Infonnation Security (IJCNlS), Vol. 3, No. I, April 2011

[6] Sun B, Guan Y, Chen J, Pooch UW , Detecting *Black-hole Attack in Mobile Ad Hoc Networks*, 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003.

[7] Mistry N, Jinwala DC, IAENG, Zaveri M, *Improving AODV Protocol Against Blackhole Attacks*, International MultiConference of Engineers and Computer Scientists IMECS Hong Kong, Vol. 2, pp 1-6, 17-19 March, 2010.

[8] Wang W, Bhargava B, Linderman M, *Defending against Collaborative Packet Drop Attacks on MANETs*. 2nd International Workshop on Dependable Network Computing and Mobile Systems, New York, USA, 27 September 2009.
[9] Salish Salem Ramaswamy, Shambhu Upadhyaya, *Proceedings of the 2006 IEEE Workshop on Information Assurance*, United States Military Academy, West Point, NY
[10] Tanu Preet Singh, Prof. R.K Singh, Jayanl Vats, Manmeel Kaur, *International Conference on Computer Science and Information Technology (lCCSIT'20 II)* Pattaya, December 2011
[11] C. E. Perkins, E.M. Royer , *Ad-hoc on-demand distance vector routing,Mobile Computing Systems and Applications*, 1999. Proceedings ,WMCSA '99. Second IEEE Workshop on, vol., no., pp.90-100, 25-26 Feb 1999.
[12] C. E. Perkins, E.M.B .Royer, S. Das , *Ad hoc on-demand distance vector (AODV) routing*, IETF Internet Draft, MANET working group, Jan.2004.
[13] H. Deng, W. Li, and D.P. Agrawal, Routing *security in wireless ad hoc networks*, Communications Magazine, IEEE, vol.40, no.10, pp. 70- 75, October 2002
[14] H. Deng, W. Li, and D. P. Agrawal, *Routing security in ad hoc networks*, IEEE Communications Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002.
[15] Y. C. Hu, A. Perrig, and D. B. Johnson, *Ariadne: A secure on-demand routing protocol for ad hoc networks*, in Eighth Annual International Conference on Mobile Computing and Networking (Mobi- Com 2002), pp. 12-23, Sept. 2002.
[16] Y. C. Hu, D. B. Johnson, and A. Perrig, *SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks*, in The 4th IEEE Workshop on Mobile Computing Systems & Applications, pp. 3 -13, June 2002.
[17] M. A. Shurman, S. M. Yoo, and S. Park, *Black hole attack in wireless ad hoc networks*, In: Proceedings of the ACM 42nd Southeast Conference (ACMSE'04), pp 96-97, Apr. 2004.FLEXChip Signal Processor (MC68175/D), Motorola, 1996.
[18] Y. A. Huang and W. Lee, *Attack analysis and detection for ad hoc routing protocols*, in The 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), pp. 125-145, French Riviera, Sept. 2004.
[19] Deng H., Li W. and Agrawal, D.P., *Routing security in wireless ad hoc networks*, Communications Magazine, IEEE, vol.40, no.10, pp. 70- 75, October 2002.
[20] Mohammad Al-Shurman et. Al, *Black Hole Attack in Mobile Ad-Hoc Network*, ACMSE'04, Apri l 2-3, 2004, Huntsville, AL, USA .
[21] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipthey, and Yoshiaki Nemoto, *Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method*, International Jtheynal of Network Securi ty, Vol.5, Issue 3, pp: 338–346, 2007

