Volume 4, Issue 9, September 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Survey on Black Hole Detection and Prevention in MANET

Ms. Twincle G. Vyas
Department of Computer Engineering
Faculty of Engineering Technology & Research
Gujarat Technological University (GTU)
Gujarat, India

Mr. Dhaval J. Rana
Department of Computer Engineering
Faculty of Engineering Technology & Research
Gujarat Technological University (GTU)
Gujarat, India

Abstract— Mobile ad hoc network (MANET) is a self-implemented network of mobile nodes formed anytime and anywhere without the help of a centralized management. Due to the open medium, dynamic network topology, autonomous terminal, lack of centralized monitoring and lack of management point Mobile Ad-hoc network are highly vulnerable to security attacks compared to wired network or infrastructure-based wireless network. In black hole attack, a malicious node gives false information of having shortest route to the destination node so as to get all data packets and drops it. In this paper, we have discussed different types of black hole attack detection and prevention techniques.

Keywords— AODV, Black hole attack, MANET, Routing protocols, malicious node.

I. INTRODUCTION

MANET consists of a collection of wireless mobile nodes that have capability to communicate with each other without use of network infrastructure or any centralized administration. Also security is important to provide protection over communicating nodes in an environment. Although security has long been a most demanding research topic in wire line networks, the unique characteristics of MANETs present a new set of challenges to security design. Routing protocol in MANET is divided into two main categories, proactive and reactive. In proactive routing protocols, routing information of nodes is exchanged, periodically, such as DSDV. In on-demand routing protocols, route is established and nodes exchange routing information when needed such as AODV [1]. Furthermore, some ad-hoc routing protocols are a combination of above categories. AODV protocol is preferred as compare to other protocols because it minimizes the routing overhead [2].AODV provides loop free routes and repair broken links [2]. AODV is an on demand routing protocol, this means that routes are only established when needed. The black hole attack is the most severe security attacks which can significantly disrupt the communications across the network. AODV protocol use control messages to find a route from source to the destination node in the network. There are three types of control messages in AODV; these are Route Request Message (RREQ), Route Reply Message (RREP), and Route Error Message (RERR).This paper presents various methods to detect and prevent Black hole attack.

II. WHAT IS BLACK HOLE ATTACK?

A Black Hole attack [16] is a kind of denial of service attack where a malicious node gives false information of having shortest route to the destination in order to get all the data packets and drop it . In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it[22]. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to other unknown address[23].The method how malicious node fits in the data routes varies. Fig. a shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node the n it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will starts Sidding data packets to node "C". In this way all the data packet will be lost consumed or lost.

Figure A. Black hole attack in

III. TECHNIQUES FOR DETECTION OF BLACK HOLE ATTACK IN MANET

A) B.Yu [6] proposes a method to detect selective forwarding attacks based on checkpoints. Firstly choosing some nodes along the path randomly as the check points node, then after receiving data packets, there will generate corresponding acknowledgments and then transmit them to the upper way. If any checkpoints node doesn't get enough acknowledgments, it will generate Warning messages to the source node, so that the detection of the selective forwarding attacks can be realized. But an apparent problem exists in this process is that the nodes have to send acknowledgments

continuously, which will greatly increase the cost of the network overhead. By the way, this method can't judge whether there malicious tamper action exists.

B) Jiang [7] proposes a method to detect selective forwarding attacks, which is based on the level of trust and packet loss. After networking topology being established, when sensing data is transmitted on the path, the intermediate nodes detect and count the number of the packets they receive and send, and report the statistical results to the BS; According to these data, the BS calculates the trust level of nodes and evaluate the packet loss, so that it can determine whether this node is an active attacking node.

C) Yu and Xiao [8], proposed a scheme which uses a multi-hop acknowledgment scheme to launch alarms by obtaining responses from intermediate nodes. Each node in the forwarding path is in charge of detecting malicious nodes. If an intermediate node detects a node as malicious in its downstream /upstream, then it will send an alarm packet to the source node/base station through multi-hops.

D) Sophia Kaplantzis et al [9] proposed a centralized intrusion detection scheme that uses only two features to detect selective forwarding and black hole based on Support Vector Machines (SVMs) and sliding windows. This intrusion detection is performed in the base station and hence the sensor nodes use no energy to support this added security feature. From this they conclude that the system can detect black hole attacks and selective forwarding attacks with high accuracy without depleting the nodes of their energy.

E) Brown and Xiaojiang [10] have proposed a scheme to detect selective forwarding using a Heterogeneous Sensor Network (HSN) model. The HSN consists of powerful high-end sensors (H-sensors) and large number of low-end sensors (L sensors). After deploying sensors, a cluster formation takes place with H-sensor as cluster head.

F) Xin, etal. Proposed [11] a light weight defense scheme against selective forwarding attack which uses neighbor nodes as monitor nodes. The neighbor nodes (monitoring nodes) monitor the transmission of packet drops and resend the dropped packets. They used a hexagonal WSN mesh topology.

G) Zurina Mohd Hanapi et al [12] proposed the dynamic window stateless routing protocol DWSIGF that is resilience to black hole and selective forwarding attack caused by the CTS rushing attack. Even without inserting any security mechanism inside the routing protocol, the dynamic window secured implicit geographic forwarding (DWSIGF) still promise a good defense against black hole attack with good network performance.

H) Riaz Ahmed Shaikh et al [13] proposed two new identity, route and location privacy algorithms and data privacy mechanism that addresses the challenging problem due to the constraints imposed by the sensor nodes [13], sensor networks and QoS issues. The proposed solutions provide additional trustworthiness and reliability at modest cost of memory and energy. Also, they proved that their proposed solutions provide protection against various privacy disclosure attacks, such as eavesdropping and hop by-hop trace back attacks [13].

I) Guorui Li et.al [14] has proposed the sequential mesh test based detection scheme. The cluster head node detects the packet drop nodes based on the sequential mesh test method after receiving the packet drop reports. This scheme extracts a small quantity of samples to run the test, instead of regulating the total times of test in advance. It decides whether continue the test or not based on the test result until it obtains the final conclusion. It requires less communication and computation power and shorter detection time to detect the selective forwarding attack nodes.

J) Deng-yin ZHANG et.al [15] et.al proposed a method to detect selective forwarding attacks based on digital watermarking technology. This method embeds watermark into the source data packets, which will be extracted at the base station (BS). The BS will judge whether there are malicious nodes in the transmission path by analyzing the packet loss rate from received data. Simulation results show that this method can effectively detect whether malicious nodes have discarded or tampered the contents of the packets.

IV. COMPARISON OF VARIOUS BLACK HOLE DETECTION TECHNIQUES IN MANET

Proposal name	Approach	Assumption	Philosophy
Dynamic learning system using DPRAODV	DPRAODV	Multiple black hole	Single non-black hole node detects
Cooperative black hole node detection using DRI and cross checking	AODV	Cooperative black hole	Single non-black hole node detects
Black hole node detection using two different solutions	AODV	Multiple black hole	Single as well as Multiple non-black node detects
Distributed and cooperative mechanism	AODV	Distributed & Cooperative	Cooperative detection
Detecting black hole attack on AODV-based Mobile Ad Hoc using dynamic anomaly detection.	AODV	Multiple black hole	Single non-black hole node detects
Single black hole node detection	AODV	Single black hole	Single non-black hole node detects
Prevention of black hole attack using fidelity table	Enhancement on AODV	Multiple black hole	Multiple non-black hole node

Detection using neighborhood based method	AODV	Multiple black hole nodes	Multiple non-blackhole nodes detects
Detection of black hole using DRI and Cross checking	Modified version of AODV	Multiple black hole	Multiple non-black hole nodes detect
Detecting black hole attacks in MANETs using Topology Graphs technique.	TOGBAD approach	Single black hole	Single black hole node detects

V. PREVENTION OF BLACK HOLE ATTACK IN MANET

In black hole, the attackers are getting the route request packets and say that it is having the latest and fresh route to the destination. But it is not having the route to that particular destination. Based on the MAC value, the route request packets are decrypted by the mobile nodes. It is difficult for the attacker to generate the secret key, since it should be shared among the nodes. There are some conditions that make the algorithm as efficient :After receiving the route requests from many paths, the destination will reply back to the source with the message that contains a session key (Ks) through the path based on the selection criteria. The session key will be used for encrypting /decrypting the original data .The session key is sent to the source by encrypting the session key along with security association number, query identifier, query sequence number, IP addresses of source and destination, route reply using the shared secret key of source and destination (Kst).Then all thevalues are subjected into a MAC algorithm like SHA-1 or MD5. The destination also finds the MAC values as,

M = C(Kst (RREQ, SANUM ,QID ,QSEQ , SA, DA)) SA, DA,NGIEHID1,NGIEHID2 ,.....NGIEHIDN

By receiving this message from destination, the sender can decrypt and compute a new MAC value by using this message and then the sender compares the new MAC value with the one it received from receiver. If they are same the sender assures that there are no alterations in the transmission otherwise the message will be dropped. Here the destination will store all the query sequence number that it received. By using this query sequence numbers the destination will identify the message replaying and denial of source attacks.

A) Receive Reply (RREP) Method

Parameters:

DSN – Destination Sequence Number, NID – Node ID, MN-ID – Malicious Node ID, IN- Intermediate Node, RREP- Route Reply, NHN- Next Hop Node.

Step 1: (Initialization Process)

In this if the source node (SN) does not have the route entry to the destination, it will broadcast a RREQ (Route Request) Message to discover a secure route till the Destination node.

Step 2: (Storing Process)

Any node received this RREQ either replies for the request or again broadcasts it to the network depending on the availability of fresh route to the destination and store the entire Route replies DSN in RRT.

Step 3:

When IN generates RREP and Sends to NHN
{
Table contains entry for each neighbor and Check which data is sent and which data is received from its neighbor. If reply comes back collects IP addresses of all nodes Updates route entry for destination and Table is updated.
}

Step 4: (Identify and Remove Malicious Node)

Retrieve the first entry from RRT. If DSN is much greater than SSN then discard entry from RRT as select Dest_Seq_No from table

```
If (DSN >>=Src_Seq_No)
{
MN=Node_Id
Discard entry from table
}
```


Step 5: (Node Selection Process)

* Sort the contents of RRT entries according to the DSN
* Select the NID having highest DSN among RRT entries.

Step 6: (Continue default process)

Call RREP method of default AODV Protocol. This show malicious node is identified and removed.

(1) The malicious node is identified at the Initial stage itself and immediately removed so that it cannot take part in further process.
(2) No delay = malicious node are easily identified
(3) No modification is made in other default operations of AODV Protocol.
(4) Better performance produced in little modification and
(5) Less memory overhead occurs because only few new things are added.

B) BAAP (Black hole Avoidance Protocol for wireless network)

This technique is used to avoid black hole attack without any use of special hardware and dependency on physical medium of wireless network [23]. This Protocol proposes AOMDV (Ad-hoc on demand multipath distance vector). In this Method every node maintains the legitimacy of their neighborhood nodes to form the correct path to destination node. In path discovery, an intermediate node will attempt to create a route that doesn't go through a node whose legitimacy ratio crosses the lower threshold level. To evaluate the performance of this algorithm some performance matrices are used which are Packet Delivery Ratio, Route Formation Delay, Node Speed, and Pause Time. Packet loss in AODV is more than 90% while in BAAP it is only 15.6%-21.3% in presence of 2-3 malicious nodes. In the absence of malicious node this protocol require little more time. Packet Loss increases as mobility increases.

VI. CONCLUSION

Black Hole Attack is a main security threat that degrades the performance of the routing protocol in Mobile Ad-hoc Network. Its detection and prevention is the main matter of concern to improve network quality. In this paper, we have analyzed and describe various techniques for detection and prevention of black hole attack in the Mobile Ad-hoc Network. Methods that we have discussed to detect and prevent black hole attack in MANET give better results than other security mechanism.

ACKNOWLWDGEMENT

In this paper, we survey of various detection and prevention technique of

REFERENCES

[1] "survey of black hole attack detection in mobile adhoc networks"shashi gurung, aditya kumar, krishan kumar saluja july 2013
[2] "Black hole attack in AODV routing protocol: A Review by ijarcsse "april-13
[3] "Detection and Prevention of Blackhole Attack in MANET Using ACO by IJCSNS" Sowmya K.S, Rakesh T. and Deepthi P Hudedagaddi.
[4] Luca Maria Gambardella IDSIA, Lugano, "Ant Colony Optimization for ad-hoc networks", The First MICS Workshop on Routing for Mobile Ad-Hoc Networks
[5] Dokurer, Semih."Simulation of Black hole attack in wireless Ad-hoc networks". Master's thesis,Atılım University, September 2006
[6] B Yu，B Xiao. "Detecting selective forwarding attacks in wireless sensor networks". In: Proe. of the 20th International Parallel and Dis tributed Processing Symposium, RhodesIsland, Greeee, 2006,1218-1230
[7] Jiang changyong, Zhang jianming. "The selective forwarding attacks detection in WSNs".Computer Engineering, 2009, 35(21):140-143
[8] Bo Yu and Bin Xiao. Detecting selective forwarding attacks in wireless sensor networks.In Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International, page 8 pp., 2006.
[9] Sophia Kaplantzis , Alistair Shilton , Nallasamy Mani , Y. Ahmet S¸ekercio glu ," Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines", intelligent sensors, sensor networks and information ,3rd international conference ,pg 335 –340,ISSNIP 2007.
[10] Jeremy Brown and Xiaojiang Du. Detection of selective forwarding attacks in heterogeneous sensor networks. In ICC, pages 1583–1587, 2008
[11] Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming, and Wang Liangmin. Lightweight defense scheme against selective forwarding attacks in wireless sensor networks. pages 226 –232, oct. 2009
[12] Zurina Mohd Hanapi, Mahmod Ismail and Kasmiran Jumari, Priority and Random Selection for Dynamic Window Secured Implicit Geographic Routing in Wireless Sensor Network", American Journal of Engineering and Applied Sciences 2 (2): 494-500, 2009.
[13] Riaz Ahmed Shaikh, Hassan Jameel, Brian J. d'Auriol, Heejo Lee, Sungyoung Lee and Young-Jae Song," Achieving Network Level Privacy in Wireless Sensor Networks ",Sensors 2010, 10, 1447-1472; doi:10.3390/s100301447

[14] Guorui Li, Xiangdong Liu, and Cuirong Wang "A Sequential Mesh Test based Selective Forwarding Attack Detection Scheme in Wireless Sensor Networks"

[15] Deng-yin ZHANGa, Chao Xub, Lin Siyuan "Detecting Selective Forwarding attacks in WSNs Authors

[16] 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.

[17] "Prevention of wormhole and black hole attacks in secure vbor for mobile ad hoc networks by t. peer meera labbai,&v. rajamani"

[18] Payal N. Raj and Prashant B.Swades, "DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET" , IJCSI International Journal of Computer Science Issues, Vol. 2, 2009

[19] Latha Tamilselvan and Dr. V Sankaranarayanan,"Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007).

[20] Zhao Min and Zhou Jiliu1, "Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks", 2009 International Symposium on Information Engineering and Electronic Commerce.

[21] Elmar Gerhards-Padilla, Nils Aschenbruck, Peter Martini, "Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs Networks ," 32nd IEEE Conference on Local Computer Networks.

[22] Prevention of Black Hole Attack on MANET UsingTrust Based Algorithm by International Journal of Scientific & Engineering Research, Volume 5, Issue 5, May-2014

