IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

A Survey on Resisting Blackhole Attacks on MANETS

Bhavana K S[1], Ravi P[2]

PG Scholar, Department of CSE, VidyaVardhaka College of Engineering, Mysuru, India[1]

Assistant Professor, Department of CSE, VidyaVardhaka College of Engineering, Mysuru, India[2]

Abstract: As the technology is advancing the communication medium is also changing. The wired medium of communication is getting transformed into wireless technology. One of the main wireless technologies used today is mobile ad-hoc networks (MANETS). One of the main issues is the security. Blackhole is one of the major attacks on the MANETS. This paper provides a survey how the blackhole attack is resisted using various protocols.

Keywords: MANETS, AODV, Malicious, Blackhole resisting mechanism.

I. INTRODUCTION

A MANET is a wireless technology which is growing rapidly. It is a collection of mobile nodes without any infrastructure. In these kinds of networks the data between the source and destination is carried out from an intermediate node.

MANET is vulnerable to the various kinds of attacks because of their dynamic topology and non-centralized management security.

A blackhole attack is a denial of service attack which occurs when a malicious node interferes in the optimal path in which the data is being transferred between the source and destination. The malicious node will consume all the packets or the data is lost.

II. RESISTING BLACKHOLE ATTACKS ON MANETS

AODV (Ad-hoc On-Demand Distance Vector Routing protocol) is a source initiated on demanding routing protocol. In this case it uses sequence numbers to identify the path to the destination.

In blackhole attack the attacker creates a RREP (revere route request packet) which will be having a highest sequence numbers of the receiver node. The sender believes this node as a normal node and starts communicating with it instead of original destination node.

Since the node sends the reply with highest sequence number and hop count the malicious nodes gets selected as one of the node among the path to the destination.

Now when the data packets are sent by source node and when it reaches the blackhole node it drops all the packets rather forwarding them to the destination, which may cause denial of service (DOS) attack.

M. Zapata [1] in the year 2002 proposed a protocol called SAODV- Secure Ad-hoc on Demand Routing Protocol which is the enhanced version of the AODV protocol. This protocol includes the digital signature and key management system which generates the key.
This uses asymmetric cryptography to authenticate all mutable nodes. But this solution had a problem of issuing the certificate authorization among the Adhoc nodes is a huge overhead. This solution may be ineffective for network when there are partitions in the node and mobility is high. The next problem occurs is that when a public key distribution happens it should have some identity to the node.

S. Lee [2] in the year 2007 proposed a solution that a modified AODV routing protocol by introducing two new parameters called as the route confirmation packets(CRQ) and route confirmation reply(CREP). According to this mechanism, an intermediate node has to send request to its next hop neighbor, upon receiving this node has to send reply and has to confirm the validity of the path by comparing the path in route reply and confirmation reply and both

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

the results are appropriate that particular route will be approved. One of the main drawbacks of this method is that if a cooperative blackhole attack occurs it cannot avoid the attack.

L. Tamilselvan [3] proposed a solution that uses a fidelity table in which each participating node is assigned with a fidelity level which determines node reliability. The source node will select the node with highest fidelity number and forwards the data. The destination node will send the acknowledgement upon receiving the data. The source node either increments or decrements the fidelity values based on the receiving or missing the acknowledgements. If the level becomes 0 then that node is marked malicious. The main drawback of this solution is high end to end delay when the malicious node is far away from the source node.

N Mistry [4] in the year 2010 introduced a solution that depends on analyzing all received route reply. Since the source receives the replies it waits for few seconds to receive multiple route replies. The source stores all the replies received in the table and rejects the nodes which are having highest sequence value considering it as a malicious node. But this solution introduces the end to end delay since source node has to wait for the multiple replies.

Seryvuth Tan [5] in the year 2013 proposed a mechanism called as Secure Route Discovery for the blackhole attacks on AODV. In this solution the source node and the destination node has to verify the sequence numbers in the request and the reply messages and also can use the cryptographic ways to exchange the information.

Kshirsagar Durgesh [6] in the year 2013 proposed a mechanism for detecting and resisting a blackhole attack called as promiscuous mode. In this approach neighbor node maintains two records i.e. forward count and receive count used for counting number of packets forwarded and received. The count will be incremented while it forwards and if the received node forwards it further then it decrements the count. The neighbor node will keep on forwarding until the count becomes 0 and that node will be treated as malicious node.

Moharlalpriya and Krishnamurthi [7] in 2014 proposed a new modified protocol called as
Modified Dynamic Source Routing Protocol(MDSR). In this approach first the source node picks the shortest path for the actual transmission or to forward the packets. Next the packet count and the transmitted data are compared, if there are any difference is there then it informs all its immediate neighbors to that there is hidden or malicious node is present in the network.

Syed U H, Afrin Iqbal and Farhan Khurshid [8] in 2014 proposed a mechanism for the resisting a blackhole attack using AODV protocol which uses Route Legitimacy value which will be attached in the route reply which will be stored in a table. A validity check is made at the receiving node which returns the valid value of the route and makes a secure entry in the routing table with less overhead.

Harsh Pratap Singh [9] in the year 2014 proposed a mechanism to discover and prevent the cooperative blackhole attack in AODV protocol using broadcast synchronization. In this solution the time sequence of the internal and external clocks with the threshold time clock. If the time exceeds this threshold value then that particular node is blacklisted.

Ruo Jun Cai [10] in the year 2014 proposed a concept called as Extended Neighbor Connectivity Based Trust Scheme in which periodically broadcasts a hello message to two hop neighbors. Once the source receives reply from three hops it will search for the information in the table called NCIT to verify that the node1 and node2 are intermediate and whether the information can be delivered in two hops. If the data is not consistent then it drops the trust level and marks as malicious node.

Raushan Kumar [11] in the year 2015 proposed a mechanism which says that the modification of AODV protocol at source and destination where the secure route discovery verifies the sequence numbers in the route request and route reply and compare the threshold values.

Nidhi Choudary [12] in the year 2015 proposed a solution to detect the malicious node or attacker by using timer based detection. In this method each node defines a trust value for its neighbor node and inserts a timer with each packet and if the trust value decreases below the threshold value for any node then all the other nodes will put that node in their blacklist.

Miss Bhandare [13] in the year 2015 proposed an approach in which the intruder will be removed through the Malicious node detection system which uses details like timestamp, time delay, hop count and IP address. This method

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

improved the performance up to 76 to 99%. The advantage of this method is that decision about the unsafe route is independently taken by the source and no other additional head is required.

Ayesha Siddiqua [14] in the year 2015 proposed an approach using secure knowledge algorithm in which it used the promiscuous mode to ensure data delivery to receiver node. In this approach AODV protocol is modified so that every node in the network will compare the node information stored in its tables the details like TTL, destination address and other details. If the entries in the table i.e. is the forward entry doesn't match with the threshold value then it is trusted and if it reaches the threshold value then it is considered as blackhole attack.

Mohamed A Abdelshafy [15] in the year 2016 proposed a mechanism called BRM-AODV protocol which will detect the blackhole neighbors. This mechanism uses a Self-Protocol Trustiness that detects the malicious intruder which is accomplished by complying with the normal protocol behavior. This method stores the last three hop times for a route reply received by the destination and the delay is calculated between the request and reply divided by the hop count.

III. CONCLUSION

Blackhole attack is type of in the mobile Adhoc network which is to drop the message while the routes are being discovered. The malicious or blackhole node will send a fake route request reply to a fake source which broadcasts a fake request in the network.

From the survey we have reviewed different solutions and mechanism to resist the blackhole attacks.

REFERENCES

[1] M Zapata, N Ashokan "Securing Ad hoc Routing Protocols" , Mobile Computing and Communications Review, Volume 6, Number 3.
[2] S. Lee, B. Han, and M. Shin. Robust routing in wireless ad hoc networks. In International Conference on Parallel Processing Workshops, pages 73–78, 2002.
[3] L. Tamilselvan and V. Sankaranarayanan. Prevention of blackhole attack in MANET. In 2nd International Conference on Wireless Broadband and Ultra-Wideband Communications, pages 21–21, Aug 2007.
[4] N. Mistry, D. C. Jinwala, and M. Zaveri. Improving AODV protocol against blackhole attacks. In International MultiConference of Engineers and Computer Scientists (IMECS), pages 1–5, Hong Kong, China, March 2010.
[5] Tan, Siew-Chong, and Keecheon Kim. "Secure Route Discovery for preventing black hole attacks on AODV-based MANETs." High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC), 2013 IEEE 10th International Conference on. IEEE, 2013.
[6] Kshirsagar, Vishvas, Ashok M. Kanthe, and Dina Simunic. "Analytical approach towards packet drop attacks in mobile ad-hoc networks." Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on. IEEE, 2014.
[7] Moharlalpriya M and Krishnamurthi I. "Modified DSR protocol for detection and removal of selective blackhole attack in Manet", 2014 Comput.Electr.Eng.,40: 530-538.
[8] Syed, U-H., Arif Iqbal Umar, and Fahad Khurshid. "Avoidance of Black hole affected routes in AODV-based MANET." Open Source Systems and Technologies (ICOSST), 2014 International Conference on. IEEE, 2014.
[9] Singh, Harsh Pratap, and Rashmi Singh. "A mechanism for discovery and prevention of co-operative black hole attack in mobile ad hoc network using AODV protocol." Electronics and Communication Systems (ICECS), 2014 International Conference on. IEEE, 2014.
[10] Cai, Ruo Jun, Peter Han Joo Chong, and Cherry Ye Aung. "Poster: Trust-based routing with neighborhood connectivity to prevent single and colluded active black hole." Communications and Networking in China (CHINACOM), 2014 9th International Conference on. IEEE, 2014.
[11] Kumar, Raushan, Abdul Quyoom, and Devki Nandan Gouttam. "To mitigate black hole attack in AODV." Next Generation Computing Technologies (NGCT), 2015 1st International Conference on. IEEE, 2015.
[12] Choudhary, Nidhi, and Lokesh Tharani. "Preventing black hole attack in AODV using timer-based detection mechanism." Signal processing and communication engineering systems (SPACES), 2015 international conference on. IEEE, 2015.
[13] Bhandare, A. S., and S. B. Patil. "Securing MANET against Co-operative Black Hole Attack and Its Performance Analysis-A Case Study." Computing Communication Control and Automation (ICCUBEA), 2015 International Conference on. IEEE, 2015.
[14] Siddiqua, Ayesha, Kotari Sridevi, and Arshad Ahmad Khan Mohammed. "Preventing black hole attacks in MANETs using secure knowledge algorithm." Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on. IEEE, 2015.
[15] Mohamed A Abdelshafy and Peter J King. "Resisting Blackhole Attacks on MANETs". Consumer Communications & Networking conference on IEEE, 2016.