ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 14, December 2016

3rd National Conference on Recent Trends in Computer Science and Engineering and Sustainability in Civil Engineering (TECHSYNOD'16)

19th, 20th and 21st December 2016

Organized by

Department of CSE, MCA &CE, Mohandas College of Engineering and Technology, Thiruvananthapuram, Kerala, India

A Review on Black Hole Attack in MANETs

Anju John, Shijin Knox G U

Department of Information Technology, GEC Bartonhill, Thiruvananthapuram, Kerala, India

ABSTRACT: An ad-hoc network is a collection of mobile nodes that dynamically form a temporary network and are infrastructure less. Networks are protected using many firewalls and encryption software. But many of them are not sufficient and effective due to its limited power and mobility. The ultimate goal of the security solutions for wireless networks is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users. Black hole attack is one of the severe security threats in ad-hoc networks which can be easily employed by exploiting vulnerability of on- demand routing protocols such as Ad-Hoc On Demand distance vector (AODV). In this paper, we have surveyed and compared the existing solutions to black hole attacks on AODV protocol.

KEYWORDS: MANET, AODV, Black hole attack

I. INTRODUCTION

Mobile ad hoc network is one of the wireless network structures in which all nodes are movable and have topology which changes dynamically. It represents complex distributed system that consists of collection of wireless mobile nodes, which are connected through wireless links. MANET is group of decentralized mobile nodes which does not rely on any fixed infrastructure, so MANET is an infrastructure less ad hoc networks. In MANET nodes itself works as router for communication within the network. Due to mobility and low cost, a MANET is suitable for applications such as campus networks, military service, vehicle networks, casual meetings, disaster relief robot networks, emergency operations, maritime communications, and so on. Routing in MANETs is error prone due to mobile nodes and dynamic topology as compared to conventional routing protocols. In addition to this battery power and limited bandwidth [1] is also a challenge. Earlier researchers on route establishment in MANET have their main focus on the efficiency and assume that no node is malicious, so all nodes are trustworthy. But in present scenario more attention has been given to security threats in MANETs. Black hole attack emerges as vulnerable security threat which could disturb routing protocol.

A. ADHOC ROUTING PROTOCOL AND BLACK HOLE ATTACK

Ad hoc distance vector routing is a reactive routing protocol in MANET that offers low processing and memory overhead, quick adaptation to dynamic link conditions and low network utilization. The paucity of security contemplation in the design of AODV makes it vulnerable to black hole attacks. In single black hole attack, a malicious node claims to have freshest and shortest route to destination, attracts data packets and drops them instead of forwarding. Sometimes these malicious nodes act in coordination resulting in collaborative black hole attacks.

In AODV, the source node (SN) initiates route discovery process by broadcasting a Route request (RREQ) to its neighbors. On receiving the RREQ, an intermediate node (IN), looks up in its routing table for a fresh enough route to destination. If such a route is unavailable, IN broadcasts the RREQ. Else, it responds with a Route Reply (RREP) to the source node. However when a link failure occurs, a route error (RERR) message is sent to notify others about the same. Only an intermediate node with fresher and valid route to destination can respond to a RREQ. On receiving a RREQ, a black hole node exploits this feature by immediately sending back a malicious RREP, having destination sequence number (DSN) set to the maximum possible value and hop count set to the minimum value and hence claims to have the freshest and shortest route to destination. Since a malicious node does not even check in its routing table, it is the first node that responds to a RREQ in most cases.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 14, December 2016

3rd National Conference on Recent Trends in Computer Science and Engineering and Sustainability in Civil Engineering (TECHSYNOD'16)

19th, 20th and 21st December 2016

Organized by

Department of CSE, MCA &CE, Mohandas College of Engineering and Technology, Thiruvananthapuram, Kerala, India

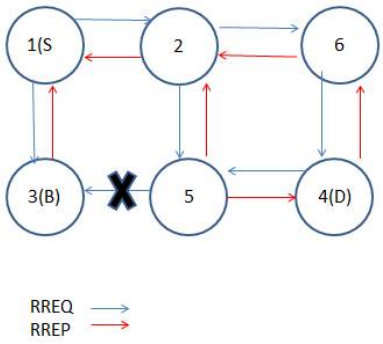

Figure 1: Black hole attack

On receiving this RREP, the source node starts routing packets via the claimed path and subsequently, the attacker node drops all the packets. Fig.1 is a pictorial representation of single black hole attack. In Fig.1, node 1 and node 4 represent the source node and the destination nodes respectively. Since node 3 is a black hole node, it hastily responds to RREQ and claims to have the freshest and shortest route to destination. On receiving this malicious RREP, node 1 delivers data packets through the path claimed by the RREP. Subsequently, node 3 drops all the packets. If there are multiple adversary nodes, the attack is called multiple black hole attack. Collaborative or cooperative black hole attack is a special case of multiple black hole attack in which two or more black hole nodes are acting in collusion.

II. TECHNIQUES FOR DETECTION AND PREVENTION OF BLACK HOLE ATTACK

A. ROUTING SECURITY IN WIRELESS AD HOC NETWORKS

Deng et.al. [3] have proposed a solution against black hole attack by modifying the AODV protocol. This approach avoids malicious nodes advertising the route that is not existed. In order to check whether the route advertised is existed and free of malicious nodes, each intermediate node has to include the address of the next hop node in RREP packets. Once the source node received the RREP packet, it extracts the details of the next hop node and sends a further request to the next hop node. This is to verify the existence of the next hope node and the routing metric value (i.e. the hop count) with the next hop node. The next hop node of the neighbor node replies the further reply packet back to the source node to confirm the route information. If the source does not receive the further reply, the route contains the malicious nodes and the route is removed from the routing table. However, this solution is vulnerable to cooperative black hole attacks. If both neighbor node and the next hop node are black hole nodes, the next hop node can response to the source node with false routing information. Therefore, this solution is still vulnerable to a cooperative black hole attack.

B. DYNAMIC LEARNING SCHEME

Satoshi Kurosawa et. al. [4] uses an anomaly detection scheme. It uses dynamic training method in which the training data is updated at regular time intervals. Multidimensional feature vector is defined to express state of the network at each node. Each dimension is counted on every time slot. It uses destination sequence number to detect attack. The feature vector include Number of sent out RREQ messages, number of received RREP messages, the average of difference of destination sequence number in each time slot between sequence number of RREP message and the one held in the list. They calculate mean vector by calculating some mathematical calculation. They compare distance between the mean vector and input data sample. If distance is greater than some threshold value then there is an attack. The updated data set to be used for next detection. Repeating this for time interval T, anomaly detection is performed.

C. NEIGHBORHOOD-BASED AND ROUTING RECOVERY SCHEME

Sun B et al [5]. Use AODV as their routing protocol and simulation is done in ns2 simulator. The detection scheme used neighborhood-based method to detect the black hole attack and then present a routing recovery protocol to build

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 14, December 2016

3rd National Conference on Recent Trends in Computer Science and Engineering and Sustainability in Civil Engineering (TECHSYNOD'16)

19th, 20th and 21st December 2016

Organized by

Department of CSE, MCA &CE, Mohandas College of Engineering and Technology, Thiruvananthapuram, Kerala, India

the true path to the destination. Based on the neighbor set information, a method is designed to deal with the black hole attack, which consists of two parts: detection and response. In detection procedure, two major steps are:
Step 1- Collect neighbor set information.
Step 2-Determine whether there exists a black hole attack.
In Response procedure, Source node sends a modify-Route-Entry (MRE) control packet to the Destination node to form a correct path by modifying the routing entries of the intermediate nodes (IM) from source to destination. This scheme effectively detects black hole attack without introducing much routing control overhead to the network. Simulation data shows that the packet throughput can be improved by at least 15 % and the false positive probability is usually less than 1.7%. The demerit of this scheme is that it becomes useless when the attacker agrees to forge the fake reply packets. This technique published in year 2003.

D. SEQUENCE NUMBER COMPARISON SCHEME

Lalit Himral et al [6] have proposed method to find the secured routes and prevent the black hole nodes (malicious node) in the MANET by checking whether there is large difference between the sequence number of source node or intermediate node who has sent back first RREP or not. Generally, the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the RRTable. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely it is from the malicious node, immediately remove that entry from the RRTable. Destination Sequence Number is a 32-bit integer associated with every route and is used to decide the freshness of a particular route.

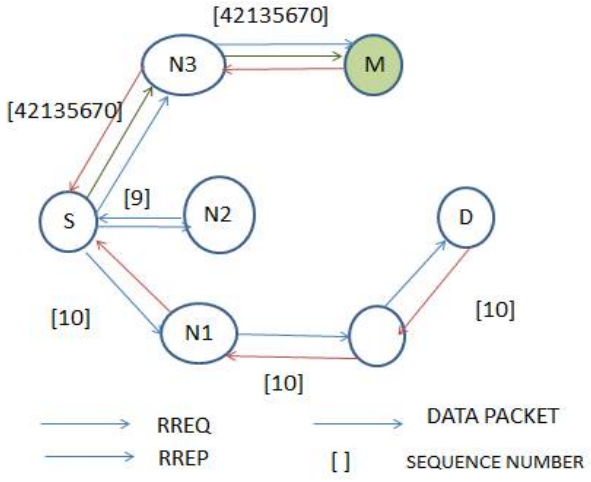

Figure 2: Sequence number scheme

The larger the sequence number, the fresher is the route. In Fig 2, Node N3 will now send it to node. Since node N1 and node N2 do not have a route to node D, they would again broadcast the RREQ control message. RREQ control message broadcasted by node N3 is also expected to be received by node M (assumed to be a malicious node). Thus, node M being malicious node, would generate a false RREP control message and send it to node N3 with a very high destination sequence number, that subsequently would be sent to the node S. However, in simple AODV, as the destination sequence number is high, the route from node N3 will be considered to be fresher and hence node S would start sending data packets to node N3. In this method before sending data packets firstly source node will check the difference between sequence numbers. If it is too large, obviously the node will be a malicious one, and it will be isolated from the network. Otherwise it simply transfers the data packets to the destination node. This solution has many advantages, it is used to maintain the identity of the malicious node as MN-Id, so that in future, it can discard any control messages coming from that node. Disadvantage is that this method cannot find multiple black hole nodes.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 14, December 2016

3rd National Conference on Recent Trends in Computer Science and Engineering and Sustainability in Civil Engineering (TECHSYNOD'16)

19th, 20th and 21st December 2016

Organized by

Department of CSE, MCA &CE, Mohandas College of Engineering and Technology, Thiruvananthapuram, Kerala, India

E. PREVENTION OF CO-OPERATIVE BLACK HOLE ATTACK IN MANET

Latha Tamilselvan et. al. [7] proposed a better solution with the modification of the AODV protocol, which avoids multiple black holes in the group. It uses Fidelity table where every node that is participating is given fidelity level that will provide reliability to that node. Any node having 0 values is considered as malicious node and is eliminated from the network. The fidelity levels of nodes are updated based on their trusted participation in the network. Upon receiving the data packets, the destination node will send an acknowledgement to the source; thereby the intermediate nodes level will be incremented. If no acknowledgement is received, the intermediate node level will be decremented. The main drawback of this solution is processing delay in the network.

F. DRI TABLE AND CROSS CHECKING SCHEME

Hesiri Weerasinghe [8] et al. proposed an algorithm to identify Collaborative Black Hole Attack. In this the AODV routing protocol is slightly modified by adding an additional table i.e. Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP). 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 to the destination node same as in the AODV. 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. If the destination replies, all intermediate nodes update or insert routing entry for that destination since we always trust destination. Source node also trusts on destination node and will start to send data along the path that reply comes back. Also source node will update the DRI table with all intermediate nodes between source and the destination. The Simulation is done in QualNet simulator. The algorithm is compared with the original AODV in terms of throughput, packet loss rate, end-to-end delay and control packet overhead. Simulation results show that the original AODV is affected by cooperative black holes and it presents good performance in terms of throughput and minimum packet loss percentage compared to other solutions.

III. OBSERVATION AND ANALYSIS

The various solutions to black hole attacks are analyzed and made a comparison based on different criteria and depicted in Table 1.

TABLE I. COMPARISION OF DIFFERENT SCHEMES

Schemes	Modifies AODV (yes/no)	Detection type	Drawbacks
Routing security scheme	Yes	Single black hole	Vulnerable to cooperative black hole attack.
Dynamic learning	No	Single black hole	High false alarm rate
Neighborhood based	Yes	Single black hole	fake reply packets forging
Sequence number Comparison scheme	Yes	Single black hole	Sequence number: limit overhead
Fidelity table	Yes	Cooperative Black Hole	delay in the network.
DRI & Crosschecking	Yes	Cooperative Black Hole	Memory overhead

IV. CONCLUSION

This paper has studied various works related to black hole attack detection mechanism in AODV-based MANETs. The prevention of black hole attacks in MANET but every proposal has its own disadvantages in their respected solutions and we made a comparison among the existed solutions. We observe that the mechanisms detects black hole node, but no one is reliable procedure since most of the solutions are having more time delay, much network overhead because of newly introduced packets and some mathematical calculations.

.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 5, Special Issue 14, December 2016*

3rd National Conference on Recent Trends in Computer Science and Engineering and Sustainability in Civil Engineering (TECHSYNOD'16)

19th, 20th and 21st December 2016

Organized by

Department of CSE, MCA &CE, Mohandas College of Engineering and Technology, Thiruvananthapuram, Kerala, India

REFERENCES

[1] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, Security in mobile ad hoc networks: challenges and solutions, Wireless Communications, IEEE, vol.11, no. 1, pp. 3847, 2004.

[2] Sathish M, Arumugam K, S.Neelavathy Pari, and Harikrishnan V S, "De- tection of Single and Collaborative Black Hole Attack in MANET,"IEEE conf. WiSPNET., pp. 2040 - 2044, September 2016.

[3] 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

[4] K H.Nakayama,S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato."A dynamic anomaly detection scheme for aodv- based mobile ad hoc networks. Vehicular Technology, IEEE Transactions on, 58(5):2471 2481, jun 2009.

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

[6] L. Himral, V. Vig, and N. Chand "Preventing aodv routing protocol from black hole attack". International Journal of Engineering Science and Technology (IJEST) Vol, 3, 2011.

[7] Latha Tamilselvan, V. Sankaranarayanan, Prevention of Co-operative Black Hole Attack in MANET, Journal of Networks, Vol 3, No 5, 13-20, May 2008

[8] Hesiri Weerasinghe and Huirong Fu, Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation, International Journal of Software Engineering and its Applica- tion, Vol.2, Issue 3, July 2008.

.