International Journal of advancement in electronics and computer engineering (IJAECE)
Volume 1, Issue 6, Sep 2012, pp.152-157, ***ISSN 2278 -1412***

A Literature Survey of Black Hole Attack on AODV Routing Protocol

Chandni Garg[1], Preeti Sharma[2], Prashant Rewagad[3]
[1] *Student, North Maharashtra University, India;*
[2] *Student, RGPV University, India;*
[3] *Student, North Maharashtra University, India;*

Abstract *- In this era of technology all the technical domains are continuously grown and develop. The evidence of this growth is different kinds of communication devices is common for all persons. As the domain of communication is grown need to provide high performance end to end reliable delivery is increases. At the same time security measures is a one of the most issue in communication system. In this project we are study different effects of Black hole attack on MANET over Ad-Hoc on Demand Distance Vector and Optimized Link State Routing protocols. Moreover it we provide the comparative study for which protocol is most of the time effecting with this attack. And finally we provide a common way to detect and prevent the black hole attack over both protocols.*

Keywords*: communication, AODV, OLSR, black hole, detection and prevention*

I. Introduction

A MANET [1], [2] is a multi-hop temporary communication network of mobile nodes equipped with wireless transmitters and receivers without the aid of any current network infrastructure. A MANET is an emerging research area with practical applications. However, A MANET is particularly vulnerable due to its fundamental characteristics [3], [4], such as open medium, dynamic topology, distributed cooperation, and constrained capability. Routing plays an important role in the security of the entire network. Thus operations in MANETs introduce some new security problems in addition to the ones already present in fixed networks. The nodes communicate by sending packets to other nodes in its radio range. The ad hoc network is characterized by a number of attributes like self organization, self-configuration, dynamic topology, restricted power, temporary network, lack of infrastructure, etc. These attributes make the ad hoc network applied in various areas, such as disaster recovery operations, smart building, military operations etc. Application fields like military operations are sensitive and prone to security attacks.

Fig. 1 Mobile Ad-Hoc Network Examples

According to the criterion that whether attackers disrupt the operation of a routing protocol or not, attacks in MANET scan be divided into two classes: passive attacks and active attacks [5], [6], [7]. In a passive attack, the attacker does not disrupt the operation of a routing protocol but only attempts to discover valuable information by listening to the routing traffic. In an active attack, however, these attacks involve actions performed by adversaries, modification and deletion of exchanged data to attract packets destined to other nodes to the attacker for analysis or just to disable the network.

II. AODV Protocol

AODV is an important on-demand routing protocol that creates routes only when desired by the source node. It maintains these routes as long as they are needed by the sources.

When a node requires a route to a destination, it initiates a route discovery process within the network. It broadcasts a route request (RREQ) packet to its immediate neighbors. Otherwise the neighbors in turn rebroadcast the request. This continues until the RREQ hits the final destination or a node with a route to the destination.

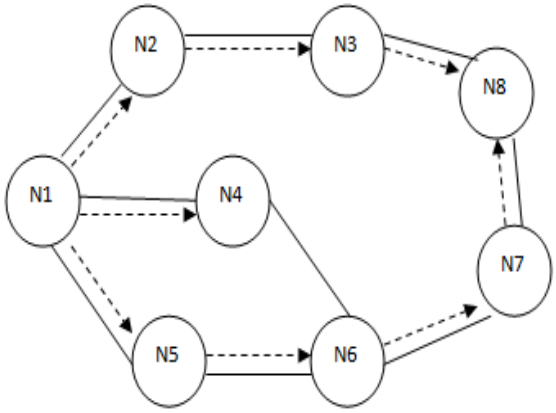
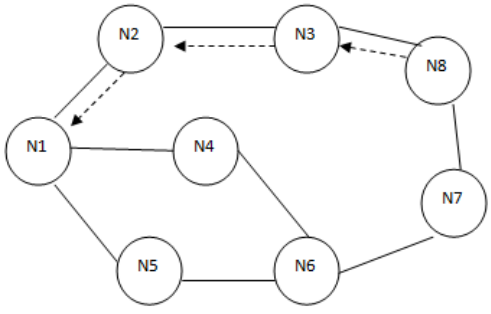


Fig 2. Propagation of RREQ

Once the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination or intermediate node responds by unicasting a route reply (RREP) packet (figure 3) back to the neighbor from which it first received the RREQ. Any intermediate node may respond to the RREQ message if it has a fresh enough route.



Fig,3.The Path of RREP

The major difference between AODV and other on-demand routing protocols is that it uses a destination Sequence number (destseqnum) to determine an up-to-date path to the destination. A node updates its path information only if the destseqnum of the current packet received is greater than the last destseqnum stored at the node.

III. Black Hole Attack

In black hole attack, the malicious node waits for its neighbor to send a RREQ packet. Upon receiving the RREQ packet, the malicious node immediately sends a forged RREP to the source node with a modified higher sequence number. In such a case, the source node assumes that the node is having a fresh route towards destination. The source node discards the RREP packets it receives from other nodes having genuine route and send data packets through malicious node. A malicious node takes all routes towards it and does not allow forwarding any packet. This attack is called black hole as it these data packets, which forms a "black hole", that is, absorbing in everything but never giving out.

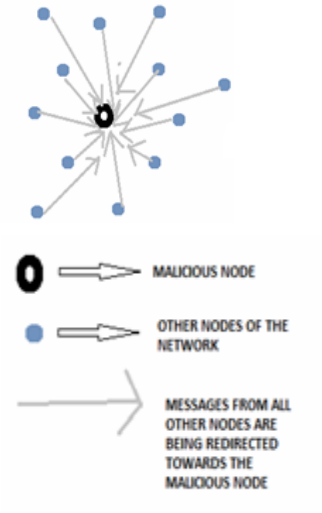


Fig.4. Black Hole Attack on MANET

IV. Problem Domain

In black hole attack, a node uses its routing protocol in order to broadcast 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. 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 the unknown address.

V. Related Work

V.1 Neighborhood-based and Routing Recovery Scheme

[1] Sun B et al. 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 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.

Advantages: This scheme effectively and efficiently 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%.

Disadvantages: 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 and the simulation is done in NS-2 simulator.

V.2 Redundant Route Method and Unique Sequence Number Scheme

[2] Shurman et al. propose two techniques to prevent the black hole attack in MANETs. The first technique is to find at least two routes from the source to the destination node. The working is as follow. Firstly the source node sends a ping packet (a RREQ packet) to the destination. The receiver node with the route to the destination will reply to this RREQ packet and then the acknowledge examination is started at source node. Then the sender node will buffer the RREP packet sent by different nodes until there are at least three received RREP packets and after identifying a safe route it transmit the buffered packets. It represents that there are at least two routing paths existing at the same time. After that, the source node identifies the safe route by counting the number of hops or nodes and thus prevents black hole attacks. In the second technique, unique sequence number is used. The sequence value is aggregated; hence it's ever higher than the current sequence number. In this technique, two values are recorded in two additional tables. These two values are last-packet-sequence-numbers which is used identify the last packet sent to every node and the second one is for the last packet received. Whenever a packet are transmitted or received, these two table values are updated automatically. Using these two table values, the sender can analyze whether there is malicious nodes in network or not. Simulation result shows that these techniques have less numbers of RREQ and RREP when compared to existing AODV.

Advantage: second technique is considered to be good compared to first technique because of the sequence number which is included to every packet contained in the original routing protocol.

Disadvantage: these both techniques fail to detect cooperative black hole attacks. Technique published in year 2004 and simulator used is ns2.

V.3 Time-based Threshold Detection Scheme

[3] Tamilselvan L et al. proposed a solution based on an Enhancement of the original AODV routing protocol. The major concept is setting timer for collecting the other request from other nodes after receiving the first request. It stores the packet's sequence number and the received time in a table named collect route reply table (CRRT). The route validity is checked based on the arrival time of the first request and the threshold value.

Advantage: the simulation shows that a higher packet delivery ratio is obtained with only minimal delay and overhead. But end-to-end delay might be raised visibly when the malicious node is away from the source node. Simulation is done in glomosim.

V.4. Random Two-hop ACK and Bayesian Detection Scheme

[4] Djenouri D et al. proposed a solution in year 2007 to monitor, detect and remove the black hole attack in manets. In the monitor phase, an efficient technique of random two-hop ack is used. Regarding the judgment issue, a bayesian approach for node accusation is used that enables node redemption before judgment. The aim of this approach is to consider and avoid false accusation attacks vulnerability, as well as decreasing false positives that might be caused by channel conditions and nodes mobility. This solution deals with all kinds of packet droppers, including as well selfish as malicious nodes launching a black hole attack. It also deals with any byzantine attack involving packet dropping in any of its steps. This solution detects the attacker when it drops packets. Simulation is done with glomosim simulator.

Advantages: the simulation results show that the random two-hop ack is as efficient as the ordinary two-hop ack in high true and low false detection, while hugely reducing the overhead. The solution utilizes cooperatively witness-based verification nevertheless, it's does not to avoid collaborate black hole attack for the judgment phase is only running on local side.

Disadvantages: it might be failed if there are multiple malicious nodes.

V.5. DRI Table and Cross Checking Scheme

[5,6] Hesiri Weera singhe 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.

Advantages: 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.

V.6. Distributed Cooperative Mechanism (DCM)

[7] Wu Chang et al. propose a distributed and cooperated "black hole" node detection mechanism which composes four sub-steps: (1) local data collection (2) Local detection (3) Cooperative detection (4) Global reaction. In local data collection, each node collects information through overhearing packets to evaluate if there is any suspicious node in its neighborhood. If finding one, the detecting node would initiate the local detection procedure to analyze whether the suspicious one is a malicious black hole node. Subsequently, the cooperative detection procedure is initiated by the initial detection node, which proceeds by first broadcasting and notifying all the one-hop neighbors of the possible suspicious node to cooperatively participate in the decision process confirming that the node in question is indeed a malicious one. As soon as a confirmed black hole node is identified, the global reaction is activated immediately to establish a proper notification system to send warnings to the whole network. Simulation is done in NS-2 simulator.

Advantage: in this DCM is compared with original AODV routing protocol. The packet delivery ratio is improved by 64.14% to 92.93% when compared with AODV.

Disadvantage: defect of this technique is a higher control overhead when compared to original AODV.

V.7. Resource-Efficient AccounTability (REAct) Scheme based on Random Audits

[8] Kozma W et al. propose a REAct scheme. This scheme provides publicly confirmable evidence of node misbehavior. REAct constitutes of three phases: (i) Audit phase, (ii) Search phase and (iii) Identification phase. The audit phase verifies the packet forwarding from audited node to the destination node. The audit phase constitutes three steps: (a) sending of an audit request. (b) Building up behavioral proof and (c) then processing of this build up behavioral proof. The search phase identifies the misbehaving links i.e., the link in which packets are dropped.

Advantage: The simulation result shows that REAct significantly reduces the communication over-head

associated with the misbehavior identification process compared to reputation-based and acknowledgment-based schemes. This reduction in resource expenditure comes at the expense of a logarithmic increase in the identification delay, due to the reactive nature of the scheme. Finally, use of binary search method exposes audit node's information to the attacker and as a result attacker can try to cheat source by dynamically changing its behavior.

V.8. Detection, Prevention and Reactive AODV (DPRAODV) Scheme

[9] In DPRAODV an additional check is done to find whether the RREP_seq_no value is higher than the threshold value as compared to normal AODV. If the RREP_seq_no value is higher than the threshold value, the node is considered to be malicious and that node is added to the black list. As the node detects a malicious node, it sends an ALARM packet to its neighbors. This ALARM packet has black listed node as a parameter. Later, if any other node receives the RREP packet it checks the black list. If that node is black listed, it simply ignores it and does not receive reply from that node again.

Advantage: The simulation result shows that the packet delivery ratio is improved as compared to AODV.

Disadvantage: Disadvantage of DPRAODV is that the routing overhead and end-to-end delay is little bit increased. And it fails with cooperative black hole attacks.

V.9. Hash based Scheme

[10] Wang W et al. propose a technique for detection of collaborative packet drop attacks on MANETs. This mechanism is for audit based detection of collaborative packet drop attacks. Firstly the vulnerability of the REAct system is studied and then illustrated that Collaborative adversary can compromise the attacker identification procedure by sharing Bloom filters of packets among them. To defend against such attacks, Wang proposed mechanism to generate node behavioral proofs. Every intermediate node needs to conduct only a hash calculation on the received packet. A collaborative attacker cannot generate its node behavioral proofs if an innocent node before it does not receive the data packets correctly.

Advantage: this approach will allow the system to successfully locate the routing segment in which packet drop attacks are conducted. No simulation is done for this technique.

V.10. Nital mistry et al.'s method

[11] mistry n et al. Proposed a solution for analyzing and improving the security of AODV routing protocol against blackhole attack. The approach basically modifies the working of source node only, using additional function pre_receivereply. A table cmg_rrep_tab, a variable mali_node and a new timer mos_wait_time are also added to the default AODV. In the proposed solution, after receiving the first rrep the source node waits for mos_wait_time and meanwhile it stores all the rreps in the cmg_rrep_tab table until mos_wait_time. In this technique the value of mos_wait_time is considered to be half the value of rrep_wait_time. Now, the source node will analyze the stored rreps and will discard the rrep which have high destination sequence number. The node which has sent these rrep with high destination sequence number are considered to be malicious node. This technique also records the identity of suspected malicious nodes as mail_node, so that in future it can discard messages coming from that node. The simulation is done in ns2 simulator. The pdr 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.11. Bait DSR (BDSR) based on Hybrid Routing Scheme

[12] Tsou P-C et al. design a novel solution named Bait DSR (BDSR) scheme to avoid the collaborative black hole attacks. The proposed solution is composed of both proactive and reactive method to make a hybrid routing protocol. The base routing protocol used is the DSR on-demand routing. Initially the source node sends bait RREQ packet. The destination address for this bait RREQ does not exists. The same method as used in DSR is used here to avoid the traffic jam problem generated by bait RREQ. The initially sent bait RREQ can attract the forged RREP and can easily remove malicious node to avoid black hole attack. In this solution the RREPs additional field records the identity of theses malicious nodes. Now the source node can easily detect the location of malicious node and will discard all the RREPs coming from that location. BDSR has an increased packet delivery ratio when compared to existing DSR and WD approach. And the communication overhead is higher than DSR routing protocol but, lower than WD approach.

References

[1] Y.-C. Hu, D. B. Johnson, and A. Perrig, "Sead: Secure efficient distance vector routing for mobile wireless ad-hoc networks," in WMCSA '02: Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications. Washington, DC, USA: *IEEE Computer Society*, 2002, . 3–13.

[2] X. Wang, T. liang Lin, and J. Wong, Feature Selection in Intrusion Detection System over Mobile Ad-hoc Network. *Technical Report,Computer Science*, Iowa State University, 2005.

[3] J. Grønkvist, A. Hansson, and M. Skøld, Evaluation of a Specification-Based Intrusion Detection System for AODV.di.ionio.gr/medhocnet07/wp content/uploads/papers/90.pdf, 2007.

[4] S. Kurosawa, H. Nakayama, and N. Kato, "Detecting blackhole attackon AODV based mobile ad-hoc networks by dynamic learning method,"*International Journal of Network Security*, pp. 338–346, 2007.

[5] K. Makki, N. Pissinou, and H. Huang, "Solutions to the black holeproblem in mobile ad-hoc network," *5th World Wireless Congress*, pp.508–512, 2004.

[6] S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.," *International Conference on Computational Intelligence and Security*, 2009.

[7] Opnet Technologies, Inc. "Opnet Simulator," Internet: *www.opnet.com*, date lastviewed: 2010-05-05

[8] M. Al-Shurman, S-M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad-HocNetworks," *ACM Southeast Regional Conf*. 2004.

[9] 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.

[10] Al-Shurman M, Yoo S-M, Park S , " Black Hole Attack in Mobile Ad Hoc Networks". *42nd Annual ACM Southeast Regional Conference* (ACM-SE'42), Huntsville, Alabama, 2-3 April 2004.

[11] Djenouri D, Badache N, "Struggling Against Selfishness and Black Hole Attacks in MANETs", *Wireless Communications & Mobile Computing* Vol. 8, Issue 6, pp 689-704, August 2008.

[12] Chang Wu Yu, Wu T-K, Cheng RH, Shun chao chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network", *Emerging Technologies in knowledge Discovery and Data Mining*, Vol. 4819, Issue 3, pp 538-549,2007.

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

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

[15] Tsou P-C, Chang J-M, Lin Y-H, Chao H-C, Chen J-L, " Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs". Paper presented at the 13th *International Conference on Advanced Communication Technology*, Phoenix Park, Korea, 13-16 Feb. 2011.