A Review on Black Hole Attack in MANETs

Himani Yadav*
M.Tech Scholar
I.T. Deptt., MMU Mullana

Rakesh Kumar**
I.T. Deptt.,
MMU Mullana

Abstract: -

Wireless networks are gaining popularity now days, as the users require wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on MANETs. Black hole attack is a security threat in which the packet is redirected to a node that actually does not exist in the network. It's an analogy to the black hole in the universe in which things disappear. In black hole attack 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. MANETs should have a secure way for transmitting packet or information over a network which is quite challenging and vital issue. In this paper, a review on different existing techniques for detection of black hole attacks with there defects is presented.

Keywords: Mobile Ad Hoc Network, DoS, Single Black Hole Attack, Collaborative Black Hole Attack.

1. INTRODUCTION

Ad-Hoc network is called Independent Basic Service Set (IBSS) Stations. IBSS communicate with each other directly and do not have any access point. Because of the mobility of nodes in ad-hoc networks, they are commonly called MANET (Mobile Ad-hoc NETwork). Mobile Ad-Hoc network [1] is a group of mobile nodes which are free to move haphazardly while being able to communicate with each other without the help of an existing network infrastructure. MANETs are suitable for use in situations where any wired or wireless infrastructure is inaccessible, overloaded, damaged or destroyed such as emergency or rescue missions, disaster relief efforts and tactical battlefields, as well as civilian MANET situations, such as conferences and classrooms or in the research area like sensor networks. MANETs eliminate this dependence on a fixed network infrastructure where each station acts as an intermediate switch. Security in MANETs is a complex issue. This complexity is due to various factors like insecure wireless communication links, absence of a fixed infrastructure, node mobility, dynamic topology and resource constraints. In mobile ad hoc networks, nodes also perform the role of routers that discover and maintain routes to other nodes in the network. The primary concern of routing protocols of MANETs is to establish an efficient and optimal route between the communicating entities. Any attack can mess up overall communication and the whole network will be destroyed. Nodes are more vulnerable to security attacks in mobile ad-hoc networks than in traditional networks with a fixed infrastructure. There are different kinds of attacks by malicious nodes that can harm a network and make it unreliable for communication. One such kind of attack is black hole attack. A black hole attack is one in which a malicious node advertises itself as having the shortest path to a destination in a network. This can cause Denial of Service (DoS) [2] by dropping the received packets. The paper is organized as follows. Section 1 discusses the introduction to MANETs. Section 2 presents Security issues for MANETs. Section 3 presents Black Hole Attack Background and different techniques of black hole attack diction and prevention is discussed in section 4. Section 5 presents the conclusion and future work.

2. SECURITY ISSUES

Security in Mobile Ad-Hoc Networks is an important concern for the network functioning. MANET often experience different security attacks because of its following features: Dynamically changing network topology, lack of central monitoring, cooperative algorithms and absence of a certification authority and etc [3, 4]. These features are explained below:

- **Dynamically changing network topology**: Nodes are free and they can move arbitrarily. So the network topology changes unpredictably and frequently, which results in change in routes, frequent partitioning of network and loss of packets.
- **Lack of centralized monitoring**: MANETs does not have any established infrastructure and centralized administration. MANET works without any preexisting infrastructure. This lack of centralized management leads MANET more vulnerable to attacks. Detecting attacks and monitoring the traffic in highly dynamic and for

large scale Ad-Hoc network is very difficult due to no central management.

- **Cooperative algorithms**: In MANET the routing algorithms need to have trust between their neighboring nodes.
- **Bandwidth constraint**: Wireless links have lower capacity as compared to the infrastructures networks.
- **Limited physical security**: Mobility of nodes results in higher security risks, which increases the possibility of spoofing, eavesdropping and masquerading and DoS attacks.
- **Energy constrained operation:** The only energy means for the mobile nodes in Ad-Hoc network is the battery power. And they also have a limited storage capacity and power.

3. BLACK HOLE ATTACK

In black hole attack [5][6], 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 [7]. 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 [8].

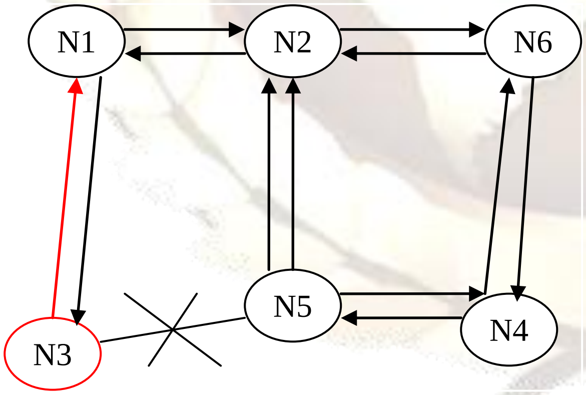

Figure 1: Black Hole Attack problem

The method how malicious node fits in the data routes varies. Figure 1 shows how Black Hole problem arises, here node "N1" want to send data packets to node "N4" and initiate the route discovery process. So if node "N3" is a malicious node then 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 "N1" before any other node. In this way node "N1" will think that this is the active route and thus active route discovery is complete. Node "N1" will ignore all other replies and will start seeding data packets to node "N3". In this way all the data packet will be lost consumed or lost.

Black hole Attacks are classified into two categories:-

3.1.1 Single Black Hole Attack [9, 10]

In Single Black Hole Attack only one node acts as malicious node within a zone. It is also known as Black Hole Attack with single malicious node.

3.1.2 Collaborative Black Hole Attack [11, 12]

In Collaborative Black Hole Attack multiple nodes in a group act as malicious node. It is also known as Black Hole Attack with multiple malicious nodes.

4. LITERATURE SURVEY

4.1.1.1 Neighborhood-based and Routing Recovery Scheme [13]

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. 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%. 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.

4.1.1.2 Redundant Route Method and Unique Sequence Number Scheme [14]

A. 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. 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. These both techniques fail to detect cooperative black hole attacks. Technique published in year 2004 and simulator used is NS2.

4.1.1.3Time-based Threshold Detection Scheme [15]

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. 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.

4.1.1.4 Random Two-hop ACK and Bayesian Detection Scheme [16]

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. 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. It might be failed if there are multiple malicious nodes. Simulation is done with GloMoSim simulator.

4.1.1.5. DRI Table and Cross Checking Scheme [17, 18]

Hesiri Weerasinghe 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.

4.1.1.6. Distributed Cooperative Mechanism (DCM) [19]

Wu Chang et al. propose a distributed and cooperated "blackhole" 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. 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. Defect of this technique is a higher control overhead when compared to original AODV.

4.1.1.7.Resource-Efficient AccounTability (REAct) Scheme based on Random Audits [20]

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. 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.

4.1.1.8. Detection, Prevention and Reactive AODV (DPRAODV) Scheme [21]

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

4.1.1.9. Hash based Scheme [22]

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. 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.

4.1.1.10. Nital Mistry et al.'s Method [23]

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.

4.1.1.11. Bait DSR (BDSR) based on Hybrid Routing Scheme [24]

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.

4.1.1.12. Bluff-Probe Based Black Hole Node Detection and prevention [25]

S Sharma et al. designed an algorithm using IERP protocol. An additional code is added for bluff probe packet and for detecting and avoiding black hole node. This algorithm is divided into following parts (i) when intra zone communication takes place. (ii) When there is inter zone communication. When intra zone communication takes place the source node broadcast bluff probe packet. This packet contains the address of nonexistent destination node. This massage is named as bluff probe request packet. The direct neighbor node receives this bluff probe packet. Now the neighbor node check their routing table entries if they have entry for this non existent destination node than they forward the packet to the next neighbor. If the node is suspected to be malicious node then they will give immediate response to the source node through the intermediate node. As it response, the source node label it as a black hole node and blocks this node. After this, the source node informs their direct neighbor for updating their routing table entries.

5. CONCLUSION AND FUTURE WORK

A Black Hole attack is one of the serious security problems in MANETs. It is an attack where a malicious node impersonates a destination node by sending forged RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node. In this paper a survey on different existing techniques for detection of black hole attacks in MANETs with there defects is presented. The detection techniques which make use of proactive routing protocol have better packet delivery ratio and correct detection probability, but have higher overheads. The detection techniques which make use of reactive routing protocols have low overheads, but have high packet loss problem. Therefore, we suggest having a hybrid detection technique which combines the advantages of both reactive and proactive routing for future research direction. Although these may not be avoided in totality, there is a need for trade-offs to achieve a secure optimal performances. Based on the above performance comparisons, it can be concluded that Black Hole attacks affect network negatively. Hence, there is need for perfect detection and elimination mechanisms. The detection of Black Holes in ad hoc networks is still considered to be a challenging task. Future work is intended to an efficient Black Hole attack detection and elimination algorithm with minimum delay and overheads that can be adapted for ad hoc networks susceptible to Black Hole attacks.

REFERENCES

1. Charles E. Perkins, “Ad Hoc Networking”, Addison- Wesley, Pearson edu., Jan. 2001.
2. Wu B, Chen J, Wu J, Cardei M , “ A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks”, Wireless Network Security. On Signals and Communication Technology. Springer, New York,2009
3. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, “Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method”, International Journal of Network Security, Vol.5, Issue 3, Nov 2007, pp 338–346.
4. Yuh-Ren Tsai, Shiuh-Jeng Wang, “Routing Security and Authentication Mechanism for Mobile Ad Hoc Networks” Chung-Shan Institute of Science and Technology, Taiwan, R.O.C., under

Grant BC-93 B14P and the National Science Council, Taiwan, R.O.C., IEEE 2004.

5. E. A .Mary Anita and V. Vasudevan, “Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Adhoc networks using Certificate Chaining”, International Journal of Computer Applications (0975 – 8887) Vol. 1, Issue 12, pp. 21-28, 2010
6. Umang S, Reddy BVR, Hoda MN, “ Enhanced Intrusion Detection System for Malicious Node Detection in Ad Hoc Routing Protocols using Minimal Energy Consumption”, IET Communications Vol.4, Issue17, pp2084–2094. doi: 10.1049/ietcom. 2009.
7. K. Biswas and Md. Liaqat Ali, “Security threats in Mobile Ad-Hoc Network”, Master Thesis, Blekinge Institute of Technology” Sweden, 22nd March 2007.
8. G. A. Pegueno and J. R. Rivera, “Extension to MAC 802.11 for performance Improvement in MANET”, Karlstads University, Sweden, December 2006.
9. N. Bhalaji and A. Shanmugam, “A Trust Based Model to Mitigate Black Hole Attacks in DSR Based Manet”, European Journal of Scientific Research, Vol.50 No.1, pp.6-15, 2011
10. Latha Tamilselvan and Dr. V Sankaranarayanan, “Prevention of Blackhole Attack in MANET”, The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 0-7695-2842-2/07, 2007.
11. Chang Wu Yu, Tung-Kuang Wu, Rei Heng Cheng, and Shun Chao Chang, “A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks”, PAKDD 2007 Workshops, LNAI 4819, pp. 538–549, 2007
12. Santhosh Krishna B V, Mrs.Vallikannu A.L , “Detecting Malicious Nodes For Secure Routing in MANETS Using Reputation Based Mechanism” International Journal of Scientific & Engineering Research, Vol. 1, Issue 3, ISSN 2229-5518, December-2010.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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
19. 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.
20. Kozma W, Lazos L , “REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits”.Second ACM Conference on Wireless Network Security, Zurich, Switzerland, 16-18 March 2009.
21. 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.
22. 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.
23. 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.
24. 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.
25. Prof. Sanjeev Sharma, Rajshree, Ravi Prakash, Vivek ,“Bluff-Probe Based Black Hole Node Detection and prevention”, IEEE International Advance Computing Conference (IACC 2009), 7 March 2009.