Black Hole Attack in Wireless Adhoc Networks

Er. Satinder Kaur
M.Tech Student
Department of Computer Science & Engineering
Amritsar College of Engineering & Technology
engg.sonia2002@gmail.com

Er. Tanu Preet Singh
Associate Professor
Department of Computer Science & Engineering
Amritsar College of Engineering & Technology
Amritsar, India
tanupreet.singh@gmail.com

Abstract - ***Wireless networks are gaining popularity to its peak today, as the users want wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET). Black hole attack is one of the security threat in which the traffic is redirected to such 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. The node presents itself in such a way to the node that it can attack other nodes and networks knowing that it has the shortest path. MANETs must have a secure way for transmission and communication which is quite challenging and vital issue. In order to provide secure communication and transmission, researcher worked specifically on the security issues in MANETs, and many secure routing protocols and security measures within the networks were proposed. The black hole attack is one of the well-known security threats in wireless mobile ad hoc networks. The intruders utilize the loophole to carry out their malicious behaviors because the route discovery process is necessary and inevitable. Many researchers have conducted different detection techniques to propose different types of detection schemes. In this paper, we survey the existing solutions and discuss the state-of-the-art routing methods. We not only classify these proposals into single black hole attack and collaborative black hole attack but also analyze the categories of these solutions and provide a comparison table***

Keywords- mobile ad hoc networks, routing protocols, single black hole attack, collaborative black hole attack

1. INTRODUCTION

Wireless mobile ad hoc network (or simply MANET throughout this paper) is a selfconfiguring network which is composed of several movable user equipment. These mobile nodes communicate with each other without any infrastructure, furthermore, all of the transmission links are established through wireless medium. According to the communication mode mentioned before. MANET is widely used in military purpose, disaster area, personal area network and so on [1]. However, there are still many open issues about MANETs, such as security problem, finite transmission bandwidth [2], abusive broadcasting messages [3], reliable data delivery [4], dynamic link establishment [5] and restricted hardware caused processing capabilities [6].The security threats have been extensively discussed and investigated in the wired and wireless networks [7], the correspondingly perplexing situation has also happened in MANET due to the inherent design defects [8]. There are many security issues which have been studied in recent years. For instance, snooping attacks, wormhole attacks, black hole attacks [9], routing table overflow and poisoning attacks, packet replication, denial of service (DoS) attacks, distributed DoS (DDoS) attacks, et cetera [10]. Especially, the misbehavior routing problem [11] is one of the popularized security threats such as black hole attacks. Some researchers propose their secure routing idea [12-15] to solve this issue, but the security problem is still unable to prevent completely.In ad hoc networks, devices rely on each other to keep the network connected. Thus, unlike traditional wireless solutions, such networks do not require any pre-existent (fixed) infrastructure, which minimize their cost and deployment time. Ad hoc networks are gaining momentum in many different application domains, like emergency, military-tactical and civilian environments. Routing protocols enable multi-hop communications in ad hoc networks. To achieve availability, routing protocols should be robust against both topology changes and malicious attacks. Existing protocol specifications cope well with the change of network topologies. However, defence against malicious attacks has remained optional. Nowadays, the trend is changing and there is an increasing interest on research focused on the provision of proposals for securing ad hoc routing protocols [1]. This research claims for methodological approaches to (i) evaluate the robustness of routing protocols against attacks and (ii) assess the effectiveness of security enhancements. This paper copes with this lack and takes a step forward to the provision of tools for auditing the security of ad hoc routing protocols. Due to space

limitations, reported research is limited to the description of how black hole attacks can be injected in proactive routing protocol-based ad hoc networks.

MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. Security is the cry of the day. In order to provide secure communication and transmission, the engineers must understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that a MANET can suffer from. A MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources.

2 AD-HOC NETWORK THREAT

In ad hoc networks devices (also called nodes) act both as computers and routers. Most routing protocols lead nodes to exchange network topology information in order to establish communication routes. This information is sensitive and may become a target for malicious adversaries who intend to attack the network or the applications running on it [1]. There are two sources of threats to routing protocols. The first comes from external attackers. By injecting erroneous routing information, replaying old routing information, or distorting routing information, an attacker could successfully partition a network or introduce a traffic overload by causing retransmission and inefficient routing. The second and more severe kind of threat comes from compromised nodes, which might (i) misuse routing information to other nodes or (ii) act on applicative data in order to induce service failures. The provision of systematic approaches to evaluate the impact of such threats on particular routing protocols remains an open challenge today.

3. ATTACK APPROACH

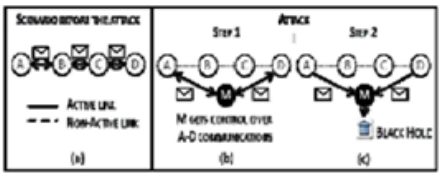
The attack approach proposed in this paper copes with the aforementioned challenge. It structures in two successive steps (see Figure 1):

1. *The malicious node (M) induces a network topology propitious for the attack success (Figure 1.b).* To cope with that goal

(i) M induces a possible routing link between attack targeted devices (call them A and D), then

(ii) M emits protocol-compliant messages for leading both A and D to choose such link for their communications.

2.M carries out the attack (Figure 1.c). In the case of a black hole attack, M drops (does not retransmit) the packets. This packet dropping can be selective (it only affects a particular type of packets) or not (all packets are black holed).

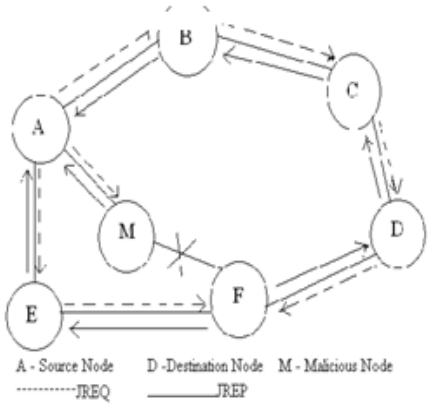


The detailed description of other type of attacks is out of the scope of this paper. However, it must be mentioned that M can carry out other type of attacks by simply changing the way it manipulates the intercepted packets (see Figure 1.c). For instance, it can forge new packets or modify, delay or reorder intercepted ones. Once the attack has been injected, its impact in the network communication and the running applications must be evaluated. This impact may, for instance, lead a particular application to fail, degrade network communications, isolate nodes or create routing loops.

4. BLACK HOLE ATTACK

Routing protocols are exposed to a variety of attacks. Black hole attack is one such attack in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the nodewhose packets it wants to intercept [3]. This attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. During the route discovery process, the source node sends route discovery packets to the intermediate nodes to find fresh path to the intended destination. Malicious nodes respond immediately to the source node as these nodes do not refer the routing table. The source node assumes that the route discovery process is complete, ignores other route reply messages from other nodes and selects the path through the malicious node to route the data packets. The malicious node does this by assigning a high sequence number to the reply packet. The attacker now drops the received messages instead of relaying them as the protocol requires. Malicious nodes take over all routes by attacking all route request messages. Therefore the quantity of routing information available to other nodes is reduced. The

malicious nodes are called black hole nodes. The attack can be accomplished either selectively or in bulk. Selective dropping means dropping packets for a specified destination or a packet every‘t’ seconds or a packet every ‘n’ packets or a randomly selected portion of packets. Bulk attack results in dropping all packets. Both result in degradation in the performance of the network.

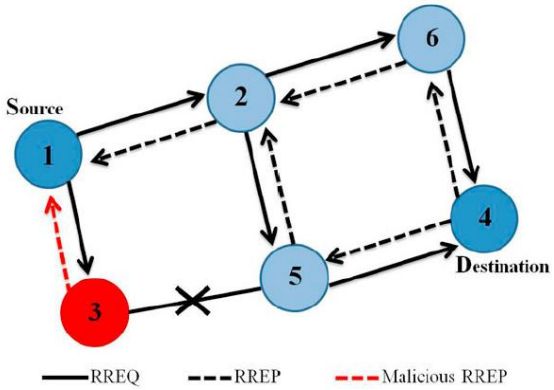


For example, source A wants to send packets to destination D, in figure1, source A initiates the route discovery process. Let M be the malicious node which has no fresh route to destination D. M claims to have the route to destination and sends join reply JREP packet to S. The reply from the malicious node reaches the source node earlier than the reply from the legitimate node, as the malicious node does not have to check its routing table as the other legitimate nodes. The source chooses the path provided by the malicious node and the data packets are dropped The malicious node forms a black hole in the network and this problem is called black hole problem.

5. SINGLE BLACK HOLE ATTACK

A black hole problem means that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbors. A single black hole attack is easily happened in the mobile ad hoc networks. An example is shown as Figure , node 1 stands for the source node and node 4 represents the destination node. Node 3 is a misbehavior node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore node 1 erroneously judges the route discovery process with completion, and starts to send data packets to node 3. As what mentioned above, a malicious node probably drops or consumes the packets. This suspicious node can be regarded as a black hole problem in MANETs. As a result, node 3 is able to misroute the packets easily, and the network operation is suffered from this problem. The most critical influence is that the PDR diminished severely. In the following, different detection schemes for single black hole attack are presented in a chronological order.

Neighborhood-based and Routing Recovery Scheme Bo Sun et al. use AODV as their routing example, and claim that the on-demand routing protocols such as DSR are also suitably applied after a slightly modified. The



detection scheme uses on a neighborhood-based method to recognize the black hole ttack, and a routing recovery protocol to build the correct path. The neighborhoodbased method is employed to identify the unconfirmed nodes, and the source node sends a Modify_Route_Entry control packet to destination node to renew routing path in the recovery protocol.In this scheme, not only a lower detection time and higher throughput are acquired, but the accurate detection probability is also achieved. To deserve to be mentioned, the routing control overhead does not increase in Bo Sun et al.’s proposal. However, this scheme is useless when the attackers cooperate to forge the fake reply packets.

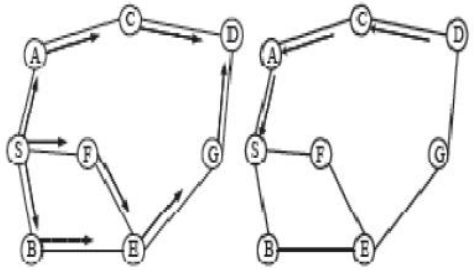
6. COOPERATIVE BLACKHOLE/ GRAYHOLE ATTACK

In the blackhole attack, the malicious node on receiving a route request from any node, falsely replies immediately with the shortest path to the destination. This way the source considers the path through the attacker as the shortest path and uses the path through attacker for all data flow between the source and destination. The attacker node can then drop all the traffic passing through it or selectively drops traffic; hence acts as a blackhole in the network. A grayhole attack is a modified form of

blackhole attack in which a node initially behaves non-maliciously but later turns malicious after gaining initial trust of other nodes; hence prevents itself from being detected easily.Most reactive routing protocols select the shortest route to destination for sending data and this property of routing protocols is exploited by adversary to create a blackhole in the network. For instance, in AODV protocol [1], when a source node S needs to send packets to a destination node D to which it has no available route, it broadcasts a Route Request (RREQ) packet to its neighboring nodes. On receiving RREQ packets, the neighboring nodes update their Routing Tables (RTs) with an entry for the source node, and checks if it is the destination node or has a fresh enough routing to the destination node. If not, then the intermediate nodes receiving a RREQ packet broadcast the RREQ to its neighbors again. The RREQ packet ultimately reaches the destination itself or at an intermediate node that has a fresh routing to the destination, which generates the Route Response (RREP) packet. The RREP packet is propagated along the reverse path to the source node.

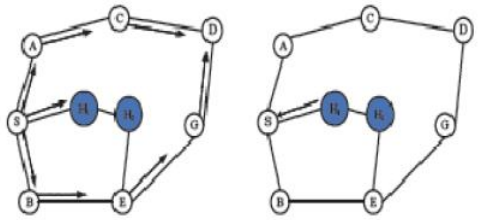
Suppose there is a malicious node in the path from source to destination, say B as shown in Fig.

1. Whenever node B receives RREQ packets, it claims that it has the shortest route to the destination node and immediately sends a false RREP packet to the source node, even though it might not be having the route to the destination.



(a) Network Flooding of RREQ (b) Propagation of RREP Message

The destination node may also send the reply but the reply from B could reach the source node first, if B is nearer to the source node. Moreover, B does not need to check its RT when sending a false message; hence its response is more likely to reach the source node firstly. This makes the source node thinks that the route discovery process is completed, ignores all other reply messages, and begins to send data packets through the path containing the attacker node.Subsequently, all the packets through B are simply consumed or lost. B could be said to form a blackhole in the network and this type of attack is known as Blackhole Attack. Deng et. al. in [3] have proposed some modifications to AODV routing protocol to prevent blackhole attacks called Security Aware AODV. In Security Aware AODV, a source node on receiving a route reply RREP packet, verifies the validity of the path with the next hop node on the route to the destination. If the next hop node either does not have a path to the node that sent the RREP or does not have a route to the destination then the node that sent the RREP is considered as malicious. However, this technique failed in the presence of multiple malicious nodes cooperating with each other. The Below figure shows when multiple blackhole nodes are acting in coordination with each other, the first blackhole node H1 refers to one of its teammates H2 as the next hop. According to Security Aware AODV, the source node S sends a further request message to ask H2 if it has a route to node H1 and a route to the destination node D. Because H2 is cooperating with H1, its further reply is "yes" to answer both the questions. So source node S starts passing the date packets. In reality, the packets are abstracted by node H1 and the security of the network is compromised.



(a) Network Flooding of RREQ (b) Propagation of RREP message

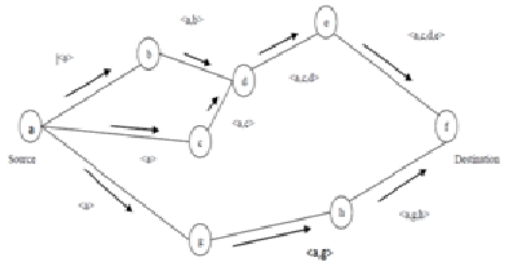
7. RELATED WORK

Several researchers have studied the vulnerabilities of ad hoc networks against black hole attacks. Deng et al [10] propose a solution to black hole problem by using one more route to the intermediate node that replays RREQ messages to check whether the route from intermediate node to destination node exists or not. This method avoids the black hole problem and prevents the network from further malicious behavior but the routing overhead is greatly increased. Also, this solution cannot prevent cooperative black hole attacks on MANETs. Al Shurman et al [11] have proposed two different solutions for black hole. The first solution suggests unicasting a ping packet from source to destination through multiple routes and then chooses a safe route based on the acknowledgement received. The second solution is based on keeping track of sequence numbers so that the black hole nodes which usually modify these sequence numbers can be detected. But these solutions have a longer delay and lower number of verified routes Marti et al

[12] have proposed a Watchdog and Pathrater approach against black hole attack which is implemented on top of Dynamic Source Routing protocol. The Watchdog module cannot detect misbehaving nodes in the presence of ambiguous collisions, receiver collisions, limited transmission power, directional antennas, false misbehavior and partial dropping. Since the system avoids the use of cryptographic methods for securing exchanged messages, it suffers from the possibility of blackmail attacks. CONFIDANT (Cooperative of Nodes, Fairness In Dynamic Adhoc NeTworks) [13] proposed by Buchegger and Le Boudec is an extended version of Watchdog and Pathrater which uses a mechanism similar to Pretty Good Privacy for expressing various levels of trust, key validation and certification. CONFIDANT allows negative ratings from other nodes resulting in false accusation. Moreover CONFIDANT does not address partial packet dropping. CORE (Collaborative Reputation)[14] is a reputation based system proposed by Michiardi et al similar to CONFIDANT. CORE consists of a set of reputation tables and a watchdog module. Each function that is monitored has a reputation table and a global RT combines the reputations calculated for different functions. The limitation with CORE is that the most reputed nodes may become congested as most of the routes are likely to pass through them. Also the limitations of the monitoring system in networks with limited transmission power and directional antennas have not been addressed in CORE.Patcha et al [15] have proposed a ollaborative architecture for black hole prevention as an extension to the watchdog method.Bansal et al [15] have proposed a protocol called OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks), which is the enhanced version of DSR protocol. CEAN uses a monitoring system and a reputation system to identify malicious nodes. But OCEAN fails to deal with misbehaving nodes properly. These papers have addressed the black hole problem on unicast routing protocols such as AODV or DSR. Our proposed scheme Black Hole Secure-ODMRP (BHS-ODMRP) is implemented on top of the route discovery process of ODMRP where in the security service is distributed over multiple nodes and nodes authenticate each other in a self organized manner.

8. PROPOSED APPROACH

In Our proposed approach, we are basically carrying our investigation for detection of Black hole node and preventing the network from this type of attack by modifying existing Dynamic Source Routing Protocol (DSR). Proposed DSR



algorithm also addresses all kinds of misbehaving nodes such as selfish or malicious nodes. Our main aim with this approach is:

- To present the various significance of MANET networks.

- To present detailed study over MANETS.

- To analyze the Blackhole attack in MANETS.

- To present approaches to provide security to the Mobile Adhoc networks from Blackhole attack.

In our approach, there exists a source node or we can call it a requester who request to its neighboring nodes that are within the transmission range of it for the route identification to the destination node. The detection Monitoring System consist of the requestor acting as a monitoring node within the network for the identification of Blackhole node. The approach on which this monitoring system nature relies assures that if a provider in the network sends back the RREP packet to the requestor more than one or two times for having route to different destinations from the same requested node and assuring that it has a shortest path to the destination than that providing node is accused as an Blackhole node. And after discovering malicious node all other neighboring nodes are informed by sending a data information packet that a particular provider is suspected as an Blackhole node in the network. So, that no other source node makes a path to the destination with this malicious node as an intermediate node.

CONCLUSION AND FUTURE WORK

Our main focus in this study is to develop the routing protocol which will handle such types of attacks and also maintaining the performance of such networks. Our approach is a new approach for the Black hole node detection within the network as the property of Black hole node allows the node to provide an assurance to the requestor of having shortest path to the destination. In this research we define an

approach with having different pairs of sources and destination such that we can identify the route from same source node to different destinations. Future work includes the simulation of this proposed approach by using NS2.34 or any other network simulator tool and also provides its performance analysis in comparison to existing routing protocols.

REFRENCES

[1] Hao Yang et al., "Security in mobile ad hoc networks: challenges and solutions**"**, IEEE Wireless Communications, Volume 11, Issue 1, Page(s): 38 – 47, Feb. 2004.

[2]. Sarma N, Nandi S (2010) Service differentiation using priority-based MAC protocol in MANETs. International Journal of Internet Protocol Technology 5(3):115–131. doi: 10.1504/IJIPT.2010.035383

[3]. Ting H-C, Chang R-S (2003) Improving the Performance of Broadcasting in Ad Hoc Wireless Networks. Journal of Internet Technology [4]:209–216 4. Liao W-H, Tseng Y-C, Lo K-L, Sheu J-P (2000) GeoGRID: A Geocasting Protocol for Mobile Ad Hoc Networks Based on GRID. Journal of Internet Technology 1(2):22–32

[5]. Yang S-J, Lin Y-C (2009) Static and Dynamic RED Tuning for TCP Performance on the Mobile Ad Hoc Networks. Journal of Internet Technology 10(1):13–21 6.

[6]. Dow CR, Lin PJ, Chen SC, Lin JH, Hwang SF (2005) A Study of Recent Research Trends and Experimental Guidelines in Mobile Ad-hoc Networks. Paper presented at the IEEE 19th International Conference on Advanced Information Networking and Applications, Tamkang University, Taiwan, 28-30 March 2005

[7]. Zhou L, Chao H-C (2011) Multimedia Traffic Security Architecture for the Internet of Things. IEEE Network 25(3):29–34. doi: 10.1109/MNET.2011.5772059

[8]. Yang H, Lou H, Ye F, Lu S, Zhang L (2004) Security in Mobile Ad Hoc Networks: Challenges and Solutions. IEEE Wireless Communications 11(1):38–47. doi: 10.1109/MWC.2004.1269716

[9]. Umang S, Reddy BVR, Hoda MN (2010) Enhanced Intrusion Detection System for Malicious Node Detection in Ad Hoc Routing Protocols using Minimal Energy Consumption. IET Communications 4(17):2084–2094. doi: 10.1049/ietcom. 2009.0616

[10] H. Deng, W. Li, and Dharma P. Agrawal, Routing Security in Ad Hoc Networks, IEEE Communications Magazine, Special Topics on Security in Telecommunication Networks, Vol. 40, No. 10, October 2002, pp. 70-75.8. Al-Shurman, M. Yoo, S. Park, Black hole attack in Mobile Ad Hoc Networks, ACM Southeast Regional Conference, 2004, pp. 96-97.

[11]. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000), Mitigating routing misbehavior in mobile ad-hoc networks, Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom), ISBN 1-8113-197-6, pp. 255-265.

[12] S. Buchegger, C. Tissieres, and J. Y. Le Boudec. A test bed for misbehavior detection in mobile ad-hoc networks –how much can watchdogs really do. Technical Report IC/2003/72, EPFL-DI-ICA, November 2003. Available on:citeseer.ist.psu.edu/645200.html.

[13]. P. Michiardi and R. Molva. Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Proceedings of the 6th IFIP Communications and Multimedia Security Conference, pages 107–121, Portorosz, Slovenia, September 2002.

[14]. A. Patcha and A. Mishra, Collaborative security architecture or black hole attack prevention in mobile ad hoc networks, Radio and Wireless Conference, 2003. RAWCON '03, Proceedings, pp. 75-78, 10-13 Aug. 2003.

[15]. S. Bansal and M. Baker. Observation-based cooperation enforcement in ad hoc networks, July 2003. Available on: http://arxiv.org/pdf/cs.NI/0307012.