COMPARISON BETWEEN BLACK HOLE ATTACK DETECTION AND PREVENTION SCHEMES IN MANET

Nishu kalia*

Kundan Munjal

Assistant Professor

Abstract:

Mobile Ad hoc Networks (MANET) is a self-configuring, infrastructure less network consists of independent mobile nodes that can communicate via wireless medium. Each mobile node can move freely in any direction, and changes their links to other devices frequently. Security is an essential part of ad hoc networks. Due to its dynamic topology, resource constraints, no centralized infrastructure and limited security, it is vulnerable to various attacks and black hole attack is one of them. In this attack, the malicious node advertises itself as having the shortest path to the destination and falsely replies to the route requests, and drops all receiving packets. In this paper, MANET's security issues, possible attacks, and comparison between different proposed schemes to detect and prevent black hole attack has been discussed.

Keywords: **MANET, Black hole attack, security threats.**

* Department of Computer Sc. & Engineering, Lovely Professional University- Punjab

Introduction:

Wireless network has been gaining popularity due to the fact that the users can communicate with each other irrespective of their geographical position. The nodes in wireless network can communicate with each other directly or via some centralized infrastructure. With centralized infrastructure, we need a central controller like base station to provide communication and authentication. But in ad hoc networks, there is direct communication between nodes without any central controller which leads to security threats. The nodes in ad hoc networks act as a host as well as router to forward the data packets. MANET is widely used in military purposes, sensor networks, rescue operations, personal area networks etc. Nodes [1] that lie within each other's range can communicate directly and are responsible for dynamically discovering each other. In order to enable communication between nodes that are not directly within each other's range, intermediate nodes act as routers that relay packets generated by other nodes to their destination.

As the topology of MANET changes frequently, it is vulnerable to various security threats. The routing protocols are exploited by the attackers with the aim to intercept the data packets. In MANET, we have three types of protocols i.e. Proactive, Reactive and Hybrid protocols. Proactive protocols (DSDV, OLSR) are table-driven protocols in which the nodes maintain and update the routing tables periodically even when there is no communication. But in reactive protocols (AODV, DSR) or On-Demand Protocols, the routes are discovered on the demand of the source node. Proactive protocols have low latency rate in discovering the route but high routing overhead. This is because the nodes periodically exchange control messages and routing table information in order to keep up-to-date routes to any active node in the network. The reactive protocols have the low routing overhead at the expense of delay to discover the route when desired by the source. Due to periodically exchange of routing information, the proactive protocols are less prone to security attacks (black hole, Sybil attack etc) as compare to reactive protocols. The control packets (Route Request, Route Reply) can be forged to intercept the normal functioning of reactive protocols. Mostly, the researchers have more focused on securing the AODV and DSR from different types of attacks and black hole attack is one of them. A lot of schemes have been proposed on detecting and preventing the black hole attack but these schemes have some pros and cons too.

Security Issues in MANET:

The various security issues in MANET are:

- **Mobility:** Each node in ad hoc network is movable. It can join or leave a network at any instant of time without informing any node. This will provide a chance to intruder to enter in the network easily and even participating in its operations.
- **Scalability:** As the nodes can join or leave the ad hoc network and can move freely, the scale of the network can be changed frequently. So scalability is a major issue concerning security. Security schemes should be able to handle a large network as well as small ones.
- **Open Wireless Medium**: An intruder can easily access this medium to gain information about the communication or can easily trap it.
- **Resource Constraint:** Every node in mobile ad hoc network has limited resources like battery, bandwidth etc. An intruder can unnecessarily waste these limited resources in order to make it unavailable to perform.
- **Broadcast Channel:** Whenever a node transmits a request, it broadcast it to every surrounding node. Any malicious node can utilize that information in a wrong manner.
- **Dynamic Network Topology:** As the nodes are highly movable in nature, so the topology changes frequently whenever the communication takes place. The communication takes place from different paths. An intruder can introduce itself in any path.
- **Lack of Centralized Administration:** Due to the lack of centralized infrastructure in MANET, it is difficult to monitor the data traffic which leads to security threats.
- **Lack of Predefined Boundary:** In MANET, the physical boundary of the network is not defined precisely. The nodes are allowed to freely move and can join or leave the network. As soon as a malicious node comes in the radio range of a node it will be able to communicate with that node.
- **Cooperativeness:** The routing protocols in MANET need the trust relationship between the neighboring nodes to discover the appropriate route. But the malicious node can disobey the routing protocols and disrupt the network

Attacks in MANET:

There are a variety of attacks possible in MANET. The attacks can be classified as active or passive attacks, internal or external attacks, or different attacks classified on the basis of different protocols.

In passive attack, the attacker does not alter the data but just snoops the data during the transmission. It includes Eavesdropping, jamming and traffic analysis and monitoring.

In case of active attacks, the attacker attempts to alter or destroy the data being exchanged in the network. This attack disrupts the normal functioning of the network. Active attacks can be classified as internal or external. In case of external attacks, the data is intercepted by the nodes that lie outside the network. But the internal attack is performed by the nodes that lie inside the network and these nodes are hard to detect. The ultimate goals of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, non-repudiation, and availability to mobile users.

The various possible attacks are:-

- **Black hole attack:** According to this attack, an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. When the attacker receives a request for a route to the destination node, it creates a reply message which advertises itself as a valid path to destination. The attacker consumes the intercepted packets without any forwarding.
- **Gray hole Attack:** The gray hole attack is also termed as misbehaving attack. In this attack, the attacker selectively drops the packet with certain probability. Also, in this attack the intruder node behaves maliciously for the time it selectively drops the packets and then switches to its normal behavior.
- **Wormhole attack:** In this attack, an attacker records the packets at one location in the network and tunnels them to another location. The routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole.
- **Byzantine attack:** In this attack, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packets which results in disruption or degradation of the routing services.
- **Information Disclosure:** An attacker may leak the confidential or important information to unauthorized nodes present in the network. The secret information may the information about network topology, geographic location of nodes or optimal routes to authorized nodes in the network.

- **Resource Consummation attack:** In this attack, an attacker attempts to consume or waste away resources of other nodes present in the network. The resources can be the battery power, bandwidth, and computational power, which are only limitedly available in ad hoc wireless networks. An attacker can consume the batteries by requesting routes and unnecessary packet forwarding to the nodes.
- **Impersonation:** In this attack, an attacker can pretend to be an authorized user and can access the secret information. The attacker may snoop information regarding the identity and authentication of the target node from the previous communication.
- **Routing Table Overflow:** In the case of routing table overflow, the attacker creates routes to nodes which do not exist. The goal is to create enough routes to prevent new routes from being created.

Cooperative Black Hole Attack:

In AODV, the RREQ (Route Request) packet is sent by the source to discover the route. If the intermediate node has the fresh enough route towards the destination, it can reply the RREP packet back to the source. Otherwise, broadcast the RREQ packet to other nodes in the network. In AODV, the sequence number is used to determine the freshness of routing information contained in the message from the originating node. If the source node receives more than one RREP packets, it will select the route with highest destination sequence number or minimum hop count. In case black hole attack, the malicious node forges the RREP packet by having the highest destination sequence number to advertise itself as a shortest path towards the destination. Then, the source node believes the malicious node and starts sending the data packets towards that node and malicious node will start dropping the data packets.

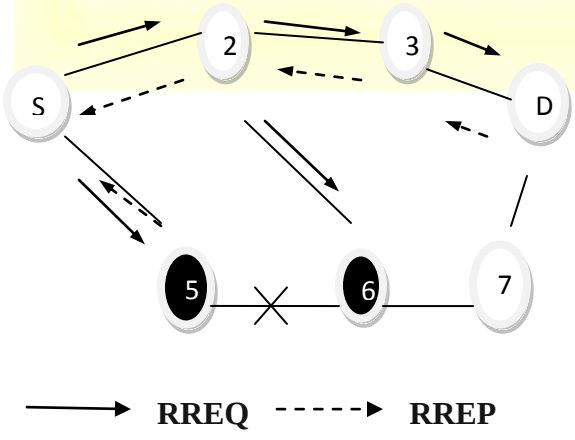

Figure 1. Cooperative Black hole Attack

The black hole attack can be performed by a single malicious node or a group of malicious nodes which works cooperatively to absorb the data packets. In the figure 1, the nodes 5 and 6 cooperatively advertise the source node to have shortest or fresh route to destination during the route discovery process and intercept the data packets.

Proposed Schemes to detect and prevent Black hole Attack in MANET:

H. Deng [4] proposed the method for detecting the single black hole node in MANET. In this method, the intermediate nodes send RREP message along with the next hop information. After getting this information, the source node sends further request to next hop node to verify that it has the route to the intermediate node or not. If the route exists, the intermediate node is trusted and source node will send data packets via that trusted node. If not, the reply message from intermediate node will be discarded and alarm message is broadcasted and isolate the detected node from network. By using this method, the routing overhead and end to end delay will be increased. If the black hole nodes work as a group in an attempt to drop packets, then this method is not efficient.

Mohammad Al-Shurman [15] proposed the two methods to avoid the black hole attacks. According to the first solution, the source node verifies the validity of the route by finding more than one route to the destination. It waits for RREP packets to arrive from more than two nodes. When the source node receives RREP packets and the routes to destination have shared hops, the source node can then recognize the safe route. This method causes routing delay. The second solution is to store the last packet sent sequence number and the last packet received sequence number in a table. When node receives reply message from another node it checks the last sent and received sequence number. If there is any mismatch, then the ALARM packet is broadcasted which indicates the existence black hole node. This mechanism is reliable and faster having no overhead.

Latha Tamilselvan [9] proposed the solution in which the source node waits for the responses including the next hop details from other neighboring nodes for a predetermined time value. When the timeout value is over, it checks in the CRRT (Collect Route Reply Table) table firstly, if there is any repeated next-hop-node or not. If in the reply paths any repeated next-hop node is present, it assumes that the paths are correct or the chance of malicious paths is limited. This solution adds a delay and the process of finding repeated next hop is an additional overhead.

Satoshi Kurosawa [2] proposed the solution based on dynamically conditions of MANET. It uses an anomaly detection scheme. The state of network at each node is expressed by multidimensional feature vector. Each dimension is counted on every time slot. The feature vector includes the number of sent out RREQ messages, number of received RREP messages, the number of received RREP messages, the average of the difference of destination sequence number in each time slot between sequence number of RREP message and the one held in the list. The mean vector is then calculated and they compare the distance between the mean vector and input data sample. If the distance is greater than some threshold value, then there is an attack. It uses dynamic training method in which the training data updated at regular intervals of time.

Payal N. Raj and Prashant B. Swadas [5] proposed DPRAODV (detection, prevention and reactive AODV) to prevent the black hole attack by informing the other nodes about the malicious node. If the value of RREP sequence number is found to be higher than the threshold value, then the node is said to be malicious and it adds the node to the black list. As the node detected an anomaly, it broadcast a new control packet, named as ALARM to its neighbors. The ALARM packet contains the black list of malicious node as a parameter, so that the neighboring nodes come to know that RREP packet from the node is to be discarded. The threshold value is the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet. The purposed solution not only detects the black hole attack, but also it tries to prevent it further, by updating the threshold which reflects the changing environment in real. The detected malicious node is then isolated from the network.

.

Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Rosilah Hassan [12] provides an improvement over the solution given in the paper [1] in which Source Intrusion Detection (SID) method is used. The SID mechanism is good for small scale MANET but when this mechanism is applied in a large scale MANET and the distance between the source node and the intermediate node is long, then the above solution is not sufficient. Secondly, if the distance between the source node and the intermediate node is long, the delay in the discovery period of the route will be high, which causes an overall network performance degradation. In order to mitigate the drawbacks in SID security routing mechanism, a new mechanism called Local Intrusion Detection (LID) security routing mechanism is proposed to allow the detection of the attacker to be locally; which means that when the suspected intermediate node unicast the RREP towards the source node, the previous node to the intermediate node performs the process of detection and not the source node.

Yiebeltal Fantahun Alem, Zhao Chenh Xuan [13] proposed an Intrusion Detection using Anomaly Detection (IDAD) technique to prevent the black hole attack. IDAD assumes every activities of a user or a system can be monitored and anomaly activities of an intruder can be identified from normal activities. Hence, by identifying anomaly activities of an adversary, it is possible to detect a possible intrusion and isolate the adversary. To do so an IDAD needs to be provided with a pre-collected set of anomaly activities, called audit data. Once audit data is collected and is given to the IDAD system, the IDAD system can compare the every activity of a host with the audit data on a fly. If any activity of a host (node) resembles the activities listed in the audit data, the IDAD system isolates the particular node by forbidding further interaction. It minimizes the extra routing packets which in turn minimizes the network overhead and facilitates faster communication.

S.Marti, T.J.Giuli, K.lai and M.bakery [14] proposed the Watchdog/Pathrater as a solution to the problem of selfish (or "misbehaving") nodes in MANET using DSR protocol. The Watchdog method is used to detect misbehaving nodes and the Pathrater, to respond the intrusion by isolating the selfish node from the network operation. Watchdog runs on each node. When a node forwards a packet, the node's watchdog module verifies that the next node in the path also

forwards the packet. The Watchdog does this by listening in promiscuous mode to the next node's transmissions. If the next node does not forward the packet, then it is considered to be misbehaving and is reported. The Path rater module uses the information generated by Watchdog to select a better route to deliver the packets, avoiding the selfish nodes.

K. Lakshmi et al [11] enhances the AODV protocol. In AODV protocol, the destination sequence number is 32-bit integer associated with every route and is used to decide the freshness of a particular route. If the sequence number is largest, the route will be fresh enough. In this method, all the sequence numbers mentioned in RREP packet is stored along with the corresponding node ID in a RR-table (Route Request). Then, if the first destination sequence number in table is much greater than the sequence number of source node. That node will be identified as malicious node and the entry will be immediately removed from the table. The proposed solution also maintains the identity of the malicious node as MN-Id, so that the control messages from that node can be discarded. In addition, there is no need to forward the control messages from that malicious node. Moreover, in order to maintain freshness, the RR-Table is flushed once a route request is chosen from it.

DRI Table and Cross Checking [16] Scheme is used to identify the cooperative black hole nodes. Each node maintains the extra DRI table with two entries 'From' and 'Through', where 1 represents for true and 0 for false. These entries stand for the information on routing data packet from and through the node. In this solution, the Intermediate node replies the next hop information and DRI entry about next hop node along with RREP packet. The source node then checks the reliability of intermediate nodes by using cross checking scheme via alternate paths by using DRI table information. It provides 50 % throughput but increases end to end delay and routing overhead.

BDSR [18] Scheme detects and avoids the black hole attack based by combining the proactive and reactive defense architecture in MANET. In this proposed solution, before the route discovery process the source node sends the bait RREQ packet which contains the virtual and non-existent destination address. To avoid the traffic jam with bait RREQ packets, all the bait RREQ packets will survive for a period time. The malicious node will send back the bait RREP

packet which advertises as the shortest path to the non-existent destination. The author adds the additional information in the bait RREP packet of having the record of generator of RREP. When source node receives the bait RREP packet, it can recognize the location of the attacker. After detecting the malicious node, a normal DSR route discovery process will be initiated. As compare to DSR and Watchdog method [14], the packet delivery ratio of this scheme is above 90%. Routing Overhead is more than DSR but lesser than Watchdog method.

Table: Comparison of different black hole detection and prevention schemes in MANET.

Proposed Schemes	Routing Protocol	Simulator	Publication Year	Results	Problems
Watchdog and Pathrater Scheme[14]	DSR	NS-2	2000	Increases throughput by 27% in network with extreme mobility	Little Routing overhead is increased as compared to normal AODV.
Single Black Hole detection scheme[2]	AODV	-	2002	Increased end to end delay and routing overhead	Unable to detect cooperative black hole nodes.
Neighborhood-based and routing recovery[19]	AODV	NS-2	2003	Probability of detecting one attacker is 93%	Cooperative Black hole nodes can forge the fake route reply packets.
Redundant route and unique sequence	AODV	NS-2	2004	Routes are verified from 75% to 98%	Detect only single black hole node and the attacker

number scheme[15]					can update the tables for last sequence number.
Dynamic learning Scheme[2]	AODV	NS-2	2007	Detection rate and false positive rate is improved.	More processing overhead needed to update the training data.
Time- based threshold detection scheme[9]	Secure AODV	GloMoSim	2007	The PDR of SAODV is around 90 to 100% when AODV is around 80%	When the malicious node is away from source node, the end to end delay increases.
Distributive Cooperative Mechanism[17]	AODV	NS-2	2007	The PDR is improved to 64.14% to 92.93% and detection rate is higher than 98%	Higher control overhead than AODV
DPRAODV[5]	AODV	NS-2	2009	The PDR is improved by 80- 85% than AODV under black hole attack	Increased routing overhead and routing overhead than AODV
Intrusion Detection[13] using anomaly	AODV	NS-2	2010	Improved throughput, less routing	More processing time is needed to compare the host

detection(IDAD)				overhead	activities with audit data.
Local Intrusion Detection[12]	AODV	GloMoSim	2011	Increased throughput, decreased end to end delay and routing overhead than scheme[4]	The routing overhead is increased than the AODV protocol.
DRI and Cross Checking Scheme[16]	AODV	NS-2	2011	The PDR is improved to 55%.	Extra database needed increased routing overhead and end to end delay.
BDSR[18]	DSR	QualNet	2011	The PDR is above 90%	Minimal overhead than DSR but lesser than Watchdog Scheme.

Conclusion:

Due to various security issues in MANET, it is vulnerable to various attacks. In this paper, we summarize and compare the proposed schemes for the detection and prevention of single and cooperative black hole attack problem. Each technique has some pros and cons. The schemes, like intrusion detection, checking reliability of nodes via neighbors, comparison of sequence numbers, cryptographic techniques (PKI, Hash-based), trust and reputation level management etc, provides the security to MANET to some extent. The comparison of these schemes is done on the basis of some parameters like end to end delay, routing overhead, throughput and packet

delivery ratio (PDR). Enhancing the security of MANET by solving the black hole attack problem is still an active area of research and much work has to be done yet. This paper will help the upcoming researchers to analyze the different techniques to prevent the black hole attack to enhance the security of the network.

References:

[1] http://cwi.unik.no/images/Manet_Overview.pdf

[2] 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.

[3] 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

[4] Hongmei Deng, Wei Li, and Dharma P.Agarwal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazine, Volume 40, Number 10, 2002, pp 70-75.

[5] Payal N. Raj and PrashantB.Swadas, "DPRAODV: A Dynamic learning system against black hole attack in AODV based MANET", International Journal of Computer Science Issues (IJCSI), Volume 2, Number 3, 2009, pp 54-59.

[6] S. Ramaswamy, H.Fu, M.Sreekantaradhya, J. Dixon, and K.Nygard, "Prevention of Cooperative black hole attack in wireless ad hoc networks," International conference (ICWN" 03), Las Vegas, Nevada, USA,2003, pp 570-575

[7] Hesiri Weerasinghe "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", Proceedings of the Future Generation Communication and Networking, Volume 2, 2008, pp 362-367

[8] N.Mistry, D.C.Jinwala and M.Zaveri, "Improving AODV protocol against black hole attacks", international multiconference of engineers and computer scientists 2010, vol 2, IMECS 2010, march 17-19 2010, Hong Kong.

[9] LathaTamilselvan and V Sankarnarayana, " Prevention of Black Hole Attack in MANET", Journal of Networks, Volume 3, Number 5, 2008, pp 13-20.

[10] E.A. Mary Anita, V. Vasudevan, "Black Hole Prevention in Multicasting Routing Protocols for Mobile Ad hoc Networks using Certificate Chaining", IJCA, Volume 1, 2011

[11] K. Lakshmi et al. "Modified AODV Protocol Against Black hole Attacks in MANET" International Journal of Engineering and Technology Vol.2 (6), 2010, 444-449.

[12] Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Rosilah Hassan "A local Intrusion Detection Routing Security over MANET Network", IEEE, July 2011, Bandung, Indonesia.

[13] Yiebeltal Fantahun Alem, Zhao Chenh Xuan, " Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anamoly Detection",2nd International Conference on Future Computer and Communication, IEEE, Volume 3, 2010

[14] S.Marti, T.J.Giuli, K.lai and M.bakery "Mitigating routing misbehaviour in mobile ad hoc networks", 6th MobiCom, Boston, Massachusetts, August 2000.

[15] Mohammad Al-Shurman, Seong-Moo Yoon and Seungjin park, "Black Hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, Proceedings of the 42nd annual southeast regional conference , 2004, pp 96-97.

[16] J.Sen ,S.Koilakonda and A.Ukil, "A mechanism for detection of cooperative black hole attack in mobile ad hoc networks", Second International Conference on Intelligent System, Modeling and Simulation ,Innovation lab, Tata consultancy services ltd. , Kolkata, 25-27January 2011.

[17] Chang Wu Yu, Tung-Kuang Wu, Rei Heng Cheng (2007) A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network. Paper presented at the PAKDD workshops, Nanjing, China, 22-25 May 2007.

[18] P-C Tsou, J-M Chang, Y-H Lin, H-C Chao, J-L Chen (2011) 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

[19] Sun B, Guan Y, Chen J, Pooch UW (2003) Detecting Black-hole Attack in Mobile Ad Hoc Networks. Paper presented at the 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003