Black Hole Attack and its Counter Measures in AODV Routing Protocol

Varsha Patidar[1], Rakesh Verma[2]
1Medicaps Institute of Technology and Management, Pigdamber, Rau (M.P)
2 Assistant Professor, CSE Department, Medicaps Institute of Technology and Management, Pigdamber, Rau (M.P)

Abstract:
Mobile Ad-Hoc network is a collection of mobile node. In this network, a wireless node usually moves randomly and dynamically forms a temporary network without a network infrastructure. Due to absence of infrastructure, MANET is used in various application like medical, battle field, business application and remote areas. MANET is vulnerable to attacks such as Black Hole Attack, Grey Hole Attack, and Worm Hole Attack. Wireless Ad- Hoc network may be unprotected against attacks by malicious nodes due to security vulnerabilities. Many mechanisms have been proposed to overcome the Black Hole Attack. A malicious node send Route Response (RREP) incorrectly of having route to destination with minimum hop count and when sender sends the data packet to this malicious node, it drops all the packet in the network. If there are multiple malicious nodes in the network, and are cooperating with each other for performing the attack than such attack is called Cooperative Black Hole Attack.

Keywords: *Black Hole Attack, Grey Hole Attack, malicious node, MANET, RREP, Worm Hole Attack.*

Introduction:

In Ad-Hoc Network, mobile nodes communicate with each other without any fixed infrastructure between them. It does not have pre-defined infrastructure to keep the network connected. Ad-Hoc Network create a network in such situation where creating the infrastructure is impossible. Destination Sequenced Distance Vector (DSDV) routing is a table driven routing protocol. In this, a routing table is maintained by each mobile node with entries of every possible destination nodes and number of hops to reach the destination node. DSDV update its routing table periodically for every change in network. Whereas, AODV is an On-Demand source initiated routing protocol when source wishes to route a packet to destination node. In all communication networks, security is the major concern, but due to dependence on other nodes for transmission, Ad-Hoc network face the greatest challenge. Many researchers have proposed solutions for mitigating and identifying the single black hole node. The packet delivery ratio will reduced if some malicious node is in the path of destination node. To overcome from this problem, identification of misbehaved nod is necessary. To improve the performance of network, trust value for node is introduced. With the help of trust value, the behavior of node can be judged. If a node has low trust value in a network, then we can identify the misbehaving node in the network. A single node or multiple nodes collectively can perform the black hole attack. When a Source node want to establish a route to Destination node, the source node S will broad cast the RREQ message to all the nodes in the network until it reaches to Destination node. This approach is followed when there is no black hole attack in the network.

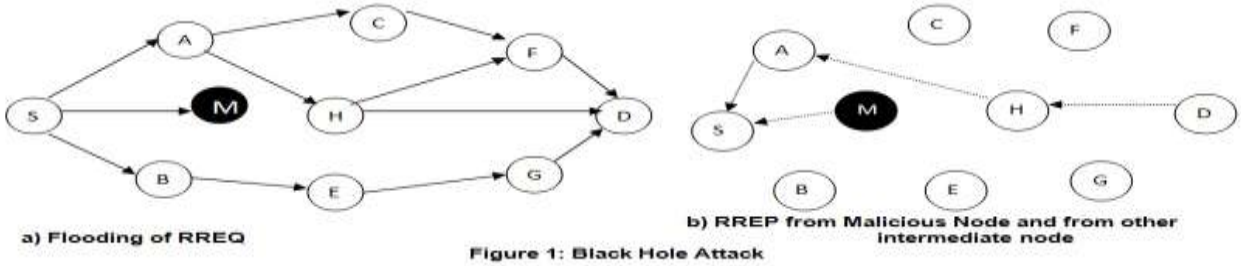

Figure 1: Black Hole Attack

In the above fig 1, when the source node broadcast the RREQ message, the black hole node will immediately reply RREQ through an RREP message. This RREP have an extremely large sequence number. Apart from this RREP, other normal nodes also receive the RREQ and destination node will select the route with minimal hop count and return the RREP. But as per AODV, largest sequence number and minimal hop count will be selected by source node. So, source node will select the black hole node for sending the data. Eavesdropping or direct dropping of received data packet is done by black hole node. Black hole node does not check its routing table and will respond to RREQ message before any other node check its routing table and respond to RREQ message.

2. AODV Routing Protocol

In proactive and reactive routing protocol, there must be good co-operation among the nodes so that the data can be routed successfully from source to destination. If nodes have good co-operation between them then there will be no packets

dropping or modification in the content. If there is no co-operation between the nodes, then there are high possibilities that an attacker take the advantage of situation and perform the malicious function. AODV routing protocol provides such situation when source node want to send the message to destination node which is not directly in contact with the source node then a route discovery process is initiated by broadcasting the RREQ message in the network. Now malicious node will take the advantage of this RREQ message and immediately send the RREP message to source node of having the route to the destination node without checking its routing table. This RREP message has the large sequence number and minimal hop count. When source node starts transmitting the data, the malicious nose will drop the packet rather than forwarding it to the destination node.

3. Co-operative Black Hole Attack

In Black Hole Attack, a node falsely advertises shortest and freshest path during route discovery process by the source node. When a group of malicious nodes works co-operatively than the condition become worse. According to Hongmei Dang et.al, [1] when source node get a RREP message of its RREQ message, from node B1 which is a malicious node, the source node sends a "further Request (FRq)" to the node B2 , asking it if it had route to destination node and also if it has route to node B1. Node B2 in response to these questions responds in YES to the source node. When source node sends a "Further Request (FRq)", it follows a different path other than node B1 and followed the path (S-3-4B2). Now source node is assured that the route S-B1-B2 is secure. Source node start sending data through node B1 and it consume the data rather than forwarding it further by compromising the security of the network.

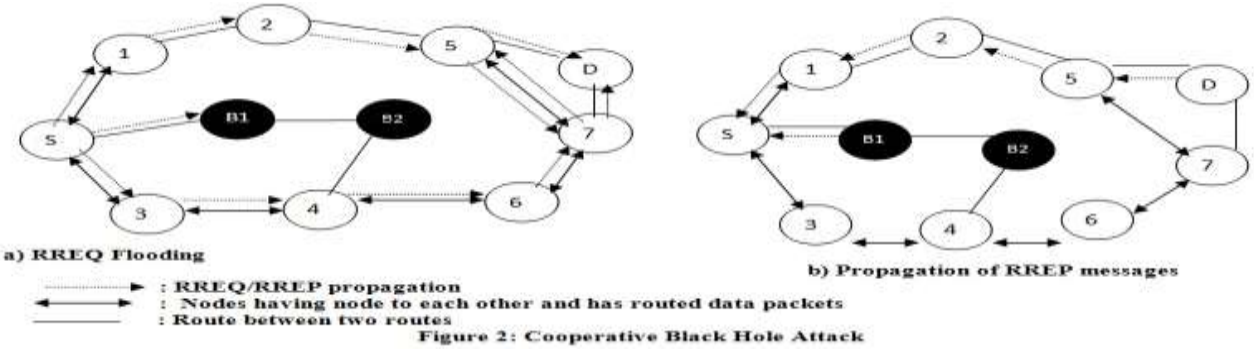

Figure 2: Cooperative Black Hole Attack

3. Related work on Black Hole Attack

There are many existing solution for detecting and mitigating the malicious node in the network. Marti et al. [2] proposed the use of watch dog and path rater. In watch dog, to detect the misbehavior in the path, it listens the transmission of the next node. In watch dog mechanism, the state information is maintained on maintained in monitored nodes, but the transmitted packets increase the memory overhead. Path rater works by keeping the rating of other nodes that ranges from 0 to 0.8 and the node that have the value 0.5 signifies as neutral. In Semih et al. [3], as the nodes are moved randomly due to this a different scenario is created by the network. Number of hopes for different path and conductivity of the network is tested. Zero hopes means there is no connection between a pair of nodes. In Buchegar [4], CONFIDANT (Cooperation of Nodes Fairness in Dynamic Ad hoc Network) was proposed. In existing watch dog and path rater scheme, this protocol adds trust manager and reputation system. The work of trust manager is based on watch dog. The trust manager works by reporting alarm to neighbor node if any malicious node is present. And this reporting is done by evaluating the events reported by watch dog. In this, with the help of trust manager, malicious node can be isolated from the network. In Ming – Yang Su et[5], they proposed that every Intrusion Detection System (IDS) node will execute a Anti Black Hole Mechanism (ABM) for estimating the suspicious value of a node by calculating the abnormal difference between RREQ and RREP message transmitted from the node.IDS will broadcast a block message if the suspicious value exceeds a thresh hold asking all nodes in the network to cooperatively isolate the malicious node with the help of this mechanism, cooperative black hole nodes can be detected in MANET. In Venkat Balakrishnan et al.[6], introduced a new mode known as secure MANET Routing with Trust Intrigue (SMRTI). This model works by capturing the evidence from neighboring node in order to identify their malicious behavior. This is also done through recommendation from other nodes in MANET. Evidence can also be captured by observing the interaction of neighbors. This model consists of two component, detection and reaction. In reaction component, whether to reject or accept a newly discovered route and also to predict the future behavior of node is done here by utilizing the evidences. In Alem Y.F et al. [7], proposed a solution based on Intrusion Detection using Anomaly Detection (IDAD) to prevent both single and multiple black hole nodes. In IDAD, it is assumed that user's activity can be monitored and this user's activity is compared with intruder's anomaly activities. A pre-collected set of anomaly activities known as audit data is provided to IDAD system and if any node activity is not listed in audit data than that node is isolated from the network. In Medadian. Met al.[8], an approach is proposed for mitigating the black hole attack. By using the opinion of neighbor node, honesty of nodes is judged. Node must show its honesty in order to transfer the data packets. The node which first receive the RREP packet, initiate the judgment process on replies and forward the packet to source. This judgment is based on opinion of network nodes about replier. After receiving the opinion of neighbor, the node

decides whether the replier is malicious node or not. The drawback of this solution is that there is no guarantee that the opinion of neighbor node is always correct. In Lalit Himral et al. [9], to find the black hole nodes, secure routes are discovered by checking the sequence number. If the difference between the sequence number of source node or intermediate (who sent first RREP) is large, then the probability of that node to be malicious is more. The first RREP by any intermediate node is usually comes from malicious node. It is recommended that such node should be immediately removed from routing table. In Michiradi et al. [10], Collaborative Reputation (CORE) protocol, each node have Reputation Table (RT) and watch dog mechanism. To implement this, there are three different levels, first one is subjective reputation, reputation is calculated from direct interaction between subject and its neighbor, second is indirect reputation, and is calculated by positive report by other nodes. Third is Functional reputation, based on behavior monitored during a specific task. These three reputations decide whether to include or exclude the node in the network.

Table1: Comparison of existing solutions to Black Hole Attack

Author's Name	Method	Disadvantage
Marti et al.	Watch Dog-detects the misbehavior in the path. Path rater- rates the other node ranges from 0 to 0.8.	Can't detect the selfish node, packet dropping and ambiguous collision in the network.
Venkat Balakrishnan et al.	SMRTI- captures evidence from neighbor by observing their behavior	Opinion of neighbor is not always correct. If malicious node increases the packet delivery ratio decreases.
Medadian et al.	Opinion from neighbor nodes and use honesty of nodes	No guarantee of neighbor's node opinion.
Buchegger et al.	CONFIDANT-Trust manager evaluates based on Watch Dog	Have complex reputation index
Michiardi et al.	CORE-Reputation based	Periodic exchange of reputation information which is unnecessary as long as node behaved well and is costly also.
Deng H et al.	Advertise if particular route exist or not by further RREQ and RREP to next node.	Cooperative Black Holes cannot be prevented, routing overhead.
Ming-Yang et al.	ABM-Estimate suspicious value by calculating RREQ and RREP difference.	Time delay and have to maintain extra data base for training data and its updations.

4. Conclusion

This paper shows various works related to black hole attack for detecting and preventing in AODV routing protocol. Various security issues of MANET are studied and as well as cooperative black hole attack is also studied. A malicious node can reduce the ratio of end to end delivery. When the suspicious value of node exceeds a thresh hold value, the detected IDS broad cast the Block message to all nodes to isolate the malicious node by all other nodes in the network. Although their exist many mechanisms for detecting black hole node but all have either more time delay or network overhead due to mathematical calculations or newly introduced packets in the network. Various proposals are given for detecting and preventing of black hole attacks by various authors. But at the same time, every proposal has its own draw back.

References

[1] Hongmei Deng, Wei Li, and Dharma P.Agarwal. Routing Security in Wireless Ad Hoc network. IEEE Communication Magzine, vol 40, no.10, October 2002.

[2] Marti S, Giuli TJ,Lai K, Baker M. Mitigating routing misbehavior in mobile ad hoc networks. International conference on mobile computing and networking, August 2000. Pp 255-265

[3] Semih Dokurer, Y.M. Erten, Can Erkin. Performance analysis of ad hoc networks under black hole attacks. IEEE Conference,pp 148-153 March 2007.

[4] Buchegger S,Boudec Le J. Performance analysis of the CONFIDANT protocol, in dynamic ad-hoc networks. ACM International symposium on mobile ad hoc networking and computing (MobiHoc'02); June 2002.pp.202-236.

[5] Ming- Yang Su, Kun- Lin Chiang, Wei Cheng Liao. Mitigation of Black Hole Nodes in Mobile Ad Hoc network. Parallel and Distributed Processing with Applications (ISPA) pp.162-167, September 2010.

[6] Venkat Balakrishnan, Vijay Varadharajan, Phillip Lues, Udaya Kiran Tupakula. Trust Enhanced Secure Mobile Ad-hoc Network Routing. 21st IEEE International Conference on AINA W 2007, Niagara Falls, Canada, pp. 27-33, May 2007.

[7] Alem, Y.F.; Zhao Cheng Xuan.Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection. Future Computer and Communication (ICFCC), 2010 2nd International Conference on , vol.3, no., pp.V3-672-V3-676, 21-24 May 2010.

[8] Medadian, M., Mebadi, A., Shahri, E. Combat with Black Hole attack in AODV routing protocol. Communications (MICC), 2009 IEEE 9th Malaysia International Conference on, vol., no., pp.530-535, 15-17, Dec.2009.

[9] Lalit Himral, Vishal Vig, Nagesh Chand. Preventing AODV Routing Protocol from Black Hole Attack. International Journal of Engineering Science and Technology (IJEST) Vol. 3 No. 5 May 2011.

[10] Michiardi, P. and Molva, R. Core. A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc Networks. In Proceeding of IFIP TC6/TC I I Sixth Joint Working Conference on Communication and Multimedia Security, 2002, 107-121.