Volume 3, Issue 12, December 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Novel Technique for a Secure Route by Detection of Multiple Blackhole Nodes in MANET

Meenakshi Sharma[1], Davinderjeet Singh[2]
CSE Department, SSCET Badhani
India

Abstract— Mobile adhoc network is a wireless infrastructure less network, in which the participating nodes act as both client and server. This helps in decentralizing the control from a single server. Mobile adhoc network is an obvious choice for deploying cost effective networks but it is also vulnerable to attacks by malicious nodes. In first place authentication and encryption can be deployed. However these also introduce extra traffic, thus pressing hard on already resource constrained MANET (limited bandwidth and processing power). This paper focuses a common security threat encountered by MANET viz. black hole attack and various approaches used to prevent this attack. Moreover a new scheme is being proposed to prevent the black hole attack in MANET which aims at decreasing end to end delay while increasing the Packet Delivery Ratio (PDR).

Keywords— MANET, bandwidth, Black hole, PDR, end-to-end delay.

I. INTRODUCTION

A mobile adhoc network (MANET) consists of a number of heterogeneous mobile nodes connected by wireless links. The high throughput and low delay of the network depends on the nodes taking part in the communication between the source and the destination. In MANETs, collection of mobile nodes may dynamically vary the topological structure. These types of networks have the salient characteristics: dynamic topologies, bandwidth constraints, variable capacity links, limited physical security and energy constrained operations. Many security threats arise because the wireless network lacks central monitoring and management of the nodes. There is common attack encountered in MANET viz. Black hole attack, which not only degrades the performance of the whole network but also results in loss of important information.

II. BLACKHOLE PROBLEM IN AODV PROTOCOL

AODV (Ad hoc On Demand Distance Vector) is an important on-demand routing protocol that creates routes only when desired by the source node. When a node requires a route to a destination, it broadcasts a route request (RREQ) packet to its neighbors, which then forward the request to their neighbors, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is located. In this process the intermediate node can reply to the RREQ (Route Request) packet only if it has a fresh enough route to the destination. Once the RREQ (Route Request) reaches the destination or an intermediate node with a fresh enough route, the destination or intermediate node responds by unicasting a route reply (RREP) packet back to the neighbor from which it first received the RREQ (Route Request). After selecting and establishing a route, it is maintained by a route maintenance procedure until either the destination becomes inaccessible along every path from the source or the route is no longer desired. A RERR (Route Error) message is used to notify other nodes that the loss of that link has occurred.

In AODV (Ad hoc On Demand Distance Vector), the sequence number is used to determine the freshness of routing information contained in the message from the originating node. When generating RREP (Route Request) message, a destination node compares its current sequence number, and the sequence number in the RREQ (Route Request) packet plus one, and then selects the larger one as RREPs (Route Request) sequence number. Upon receiving a number of RREP (Route Request), the source node selects the one with greatest sequence number in order to construct a route. But, in the presence of black hole when a source node broadcasts the RREQ (Route Request) message for any destination, the black hole node immediately responds with an RREP (Route Request) message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source assumes that the destination is behind the black hole and discards the other RREP (Route Request) packets coming from the other nodes. The source then starts to send out its packets to the black hole trusting that these packets will reach the destination. Thus the black hole will attract all the packets from the source and instead of forwarding those packets to the destination it will simply discard those. Thus the packets attracted by the black hole node will not reach the destination.

III. LITERATURE REVIEW

Jeroen Hoebeke et. al, discussed about application of mobile ad-hoc networks and the challenges being faced while using them. In this paper, a complete introduction has been given about the wireless networks. Moreover this paper provides an

insight into the potential applications of ad-hoc networks and discusses the technological challenges being faced by network and protocol designers. Most prominent of the challenges are routing, resource and service discovery and security. Different attacks pertaining to security are deletion, fabrication, replication and redirection of data packets. But despite challenges, mobile ad-hoc network opens a new business opportunity for service providers.

Mehdi Medadian et. al, proposed a novel approach for countering the black hole attack. The approach is based on using negotiations with neighbors who claim to have a route to destination. In this approach, any node uses a set of rules to decide the honesty of the reply's sender. During packet transferring, the activities of a node are logged by its neighbors. These neighbors send their opinion about a node. When a node receives replies from all neighbors, it is able to decide whether the replier is a malicious node or a legitimate node. The opinion send by neighbors is based on the number of packets sent to a particular node and number of packets forwarded by it. The method yields better percentage of packets received in presence of cooperative black hole attack.

Songbai Lu et. al, proposed a method that is effective and secure against the black hole attack in mobile ad-hoc network. This method is works on the basis of direct verification of the destination node using random number exchange. In this method, the source node sends verification packet SRREQ (Secure Route Request) to destination node along opposite direction route of RREP (Route Reply) received while the verification packet contains random number. This packet is forwarded using different routing paths. At the destination end, upon receiving two or more SRREQ (Secure Route Request) packets, their contents are checked. If content are same, verification confirm packet SRREP (Secure Route Reply) is sent to source along different routing paths. On the source end, upon receiving two or more SRREP (Secure Route Reply) packets, their contents are checked for match. If they match, the route is added to the routing table and warning message regarding malicious nodes, is propagated throughout the network. This scheme can effectively prevent black hole attack and also maintain a high routing efficiency.

Jaydip Sen et. al, proposed a novel method to defend mobile ad-hoc network against cooperative black hole attack using AODV (Ad hoc On Demand Distance Vector) routing protocol. The method used ensures reasonable throughput level in the network. The proposed algorithm uses DRI (Data Routing Information) table and cross checking mechanism to ensure security against black hole attack. The experimental results show that the proposed scheme improves the packet delivery ratio and can further be enhanced to defend mobile ad-hoc network against resource consumption attack.

Fidel Thachil and K C Shet, proposed a method to detect and mitigate malicious nodes from mobile ad-hoc network. The detection and mitigation of malicious nodes from the network is based on trust factor being calculated by every node for its neighboring nodes. This trust value is calculated by a ratio between the number of packet received by the node and number of packets dropped by it. Each node has a certain trust value. A threshold value is specified below which a node would be considered malicious and as a result the node will be deleted from the reliable routes and information regarding the malicious node is broadcasted throughout the network. This method works far better than pure AODV (Ad hoc On Demand Distance Vector) and ensures efficient packet delivery even in the presence of malicious nodes.

Kundan Munjal et. al, proposed a novel approach for detecting cooperative black hole nodes in the network and propagating information regarding malicious nodes throughout the network. For experimentation, three different scenarios are tested. In first, no malicious node is present, so the route is considered reliable for sending data. In second case, two cooperating malicious nodes are detected and information regarding them is propagated throughout the network. In third case, on finding a node to be reliable, information regarding its reliability is spread through the network. The proposed network works well in all scenarios and achieves success against black hole attack. Thus ensuring reliable route from source to destination. But the algorithm requires improvements in end-to-end delay as well as routing overhead.

Nidhi Sharma & alok Sharma, presented a couple of solutions that can be used as a strategy against the black hole attack in MANET (Mobile Ad hoc Network). First solution is to have multiple routes to destination and unicast ping packet to destination using multiple routes (assigning different packet ID's and sequence number). Upon checking the replies received from different routes, decision is made regarding the selection of a route for communication. In the second approach, sequence number is used for the verification of legitimate node. Two extra tables are maintained to record sequence number of the forwarded packets and sequence number of the received packets. If there is a mismatch between sequence number of received RREP (Route Reply) and the sequence number of the table, the route discovery process is started while alarming the whole network about the node. The scheme does not add overhead as sequence number itself is included in every packet in base protocol.

Neha Kaushik et. al, discussed the various issues surrounding the Mobile Ad hoc Network and focuses on one of the challenges issue associated with MANET viz. Black hole attack in on demand routing protocol. The proposed solution is to modify the AODV (Ad hoc On Demand Distance Vector) routing protocol to detect black hole nodes in the network and to find secure routes for the data transmission from source to destination. Firstly, two parameters are added to the routing table of each node. These are data packet sent and data packet received. Secondly, an additional table is maintained at source node to keep track of the black hole nodes which reply as early as possible against a RREQ (Route Request). The proposed method results in increased throughput and PDR (Packet Delivery Ratio) and decrease in end to end delay.

IV. PROPOSED SOLUTION

Black hole attack is the most common active type of attack. When black hole attack is encountered in the network, throughput of the network is reduced while the delay increases. The black hole attack is even worse if multiple black

holes exist in the network. All the methods discussed in various papers have their own shortcomings with respect to packet delivery, packet lost rate and end to end delay. The aim of the study is to detect the cooperative black hole attack using AODV protocol in MANET. This paper focuses on finding a secure route for communication by detecting and isolating all the malicious nodes in mobile Adhoc network. The basic behind the proposed scheme is to detect and isolate multiple black hole nodes in the network and thus ensuring increase in packet delivery ratio while decreasing end to end delay. Various performance metrics would be used for evaluating the performance of the network using the proposed scheme.

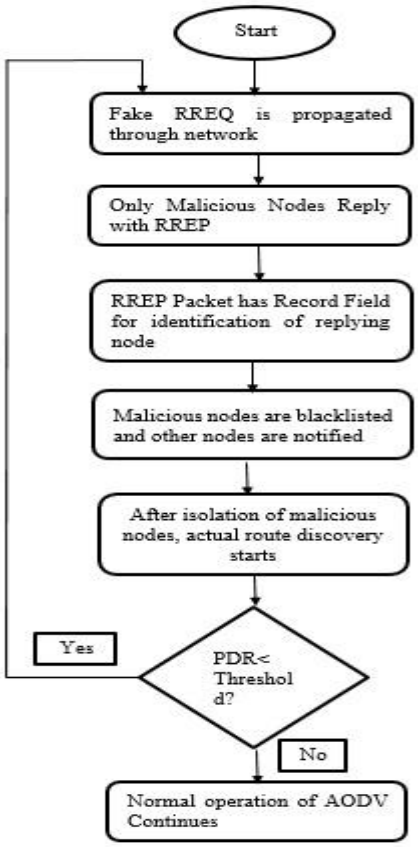

Figure:1 Methodology used

V. CONCLUSION & FUTURE WORK

Here a mechanism is proposed to provide more security in MANET after detection of the black hole nodes is done. By using fake RREQ packet and modified RREP packet, the black hole nodes are detected at the initial stage before the actual route discovery process of AODV. It leads to less routing overhead and high packet delivery ratio. In future, implementation of the proposed technique will be done using network simulator (NS2). Also testing of the new scheme against parameters like throughput and end-to-end delay will be done.

REFERNCES

[1] J. Hoebeke, I. Moerman, P. Demester and B. Dhoedt, "An Overview of Mobile Ad Hoc Network: Applications and Challenges," no. 4, pp. 60-66, 2005.
[2] M. Medadian, M. Yektaie and A. Rahmani, "Combat with Black Hole Attack in AODV Routing Protocol in MANET," IEEE, 2009.
[3] S. Lu, L. Li, K.-Y. Lam and L. Jia, "SAODV: A MANET Routing Protocol that can withstand Black Hole Attack," IEEE, pp. 421-425, 2009.
[4] J. Sen, S. Koilakinda and A. Ukil, "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad-hoc Networks," International Conference on Intelligent Systems, Modelling and Simulation, pp. 338-343, 2011.
[5] F. Thachil and K. Shet, "A Trust based Approach for AODV protocol to mitigate black hole attack in MANET," International Conference on Computing Sciences, pp. 281-285, 2012.
[6] K. Munjal, S. Verma and A. Bakshi, "Cooperative Black Hole Node Detection by modifying AODV," International Journal of Management, IT and Engineering, vol. 2, no. 8, pp. 484-501, 2012.
[7] N. Sharma and A. Sharma, "The Black Hole node attack in MANET," IEEE Second International Conference on Advanced Computing & Communication Technologies, pp. 546-550, 2012.
[8] N. Kaushik and A. Dureja, "Performance Evaluation of Modfied AODV against Blackhole attack in MANET," European Scientific Journal, vol. 9, no. 18, pp. 182-193, 2013.

