International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

Research Article

Implementation of a Novel Technique for a Secure Route by Detection of Multiple Blackhole Nodes in Manet

Meenakshi Sharma[Å] and Davinderjeet Singh[Å*]

[Å]Sri Sai College of Engineering & Technology, Badhani, Pathankot

Accepted 05 January 2014, Available online 01 February 2014, **Vol.4, No.1 (February 2014)**

Abstract

Mobile Ad hoc Networks is a self-configuring, infrastructure less network which consists of independent mobile devices that can communicate via wireless medium. Each mobile device can move freely and changes their links to other devices frequently. Security is an essential part of ad hoc networks. Without any centralized infrastructure, dynamic topology, limited security and resource constraints, it is vulnerable to various attacks and black hole attack is one of them. In black hole 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, a mechanism to detect the black hole nodes has been implemented.

Keywords*: MANET, Black hole.*

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.

AODV (Ad hoc On Demand Distance Vector) is a reactive routing protocol. Upon requirement a node broadcasts a route request (RREQ) packet to its neighboring nodes, which further forward this request to their neighbors, and continues until the intermediate node with route to destination or the destination itself receives this request packet. The intermediate node reply to the RREQ (Route Request) packet by unicasting a route reply (RREP) packet back to the neighbor from which it first received the RREQ (Route Request).

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 route to the destination. The source assumes that the destination is behind the black hole and discards the other RREP (Route Reply) packets coming from the other nodes. The source starts sending packets to the black hole and trusting that these packets will reach the destination. Thus the black hole receives all the packets from the source and instead of forwarding these packets to the destination, it simply discards these packets.

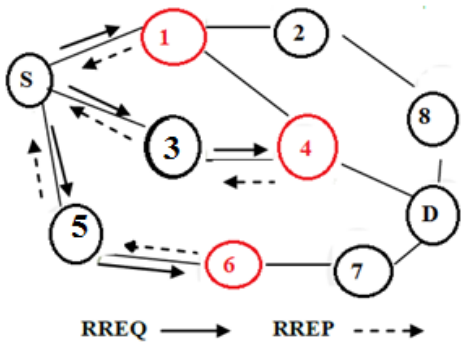

Fig 1: Black Hole Nodes in MANET

Literature Review

Mehdi Medadian et. al, proposed a novel approach based on using negotiations with neighbors for countering the black hole nodes. 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

*Corresponding author: **Davinderjeet Singh**

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.

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.

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.

Pramod Kumar Singh et. al, proposed a method that uses promiscuous mode to detect malicious node and propagates the information of malicious node to all other nodes in the network. The source node floods a RREQ (Route Request) packet in the network and waits for RREP (Route Reply) packet to have a new route to the destination node. If the RREP (Route Reply) is received from the intermediate node, the node receiving RREP (Route Reply) packet, switches its promiscuous mode and sends a hello message to destination. If the intermediate node forwards the message to destination, the node is safe. Otherwise the node is a malicious one.

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.

Meenakshi Patel & Sanjay Sharma, projected a novel automatic security mechanism using SVM (Support Vector Machine) to defend against malicious attack occurring in AODV (Ad hoc On Demand Distance Vector). This method uses three metrics viz. Packet Delivery Rate (PDR), Packet Modification Rate (PMR) and Packet Misroute Rate (PMISR), to decide the behavior of a node. The information required by the metrics is gathered from all the nodes in the network. These metrics are checked against a threshold, below which the node is considered malicious. The projected scheme is simple and provides fast and quick response to suspicious or compromised node.

M. Jhansi et. al, proposed a new method of detecting cooperative black hole attack in MANET. This method uses extra bits of information to store the information regarding the number of packets received by a node and the number of packets further transferred by it. Two bits are used. 1st bit first stands for information on routing data packet from the node while the second bit through stands for information on routing data packet through the node. Moreover a cross check is done on the intermediate node generating RREP (Route Reply) by making it to provide its next hop node and its DRI (Data Routing Information) table. The DRI entry is checked by source node and data is routed depending on a positive match. Otherwise FRq (Further request) message is send to NHN (Next Hop Node) to check the reliability of the intermediate node. This method can be applied to identify multiple black hole nodes cooperating with each other and to discover secure paths from source to destination.

Rutvij H. Jhaveri, presented a method to avoid malicious nodes from participating in the information exchange between two nodes and also reducing the network load. This method works on R-AODV (Reverse AODV), which states that a , a PEAK value is calculated by intermediate node using parameters viz. routing table sequence number, RREP sequence number and number of replies during a time interval. Maximum possible value acceptable as a sequence number is the PEAK value and if a RREP packet received, has a sequence number higher than the PEAK value, the packet is simply discarded. In this way, only genuine RREP are received at the source. Thus reducing the network traffic. This method increases the packet delivery ratio with acceptable routing overhead.

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 at steady rate. The black hole attack is even worse if multiple black holes exist in the network. 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 detection of the cooperative black hole nodes will provide more security to MANET.

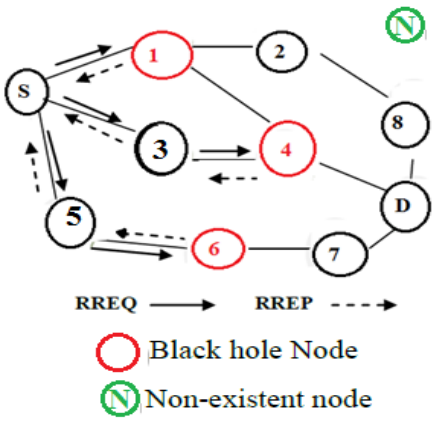

Fig 2: Sending fake RREQ packet

Results & Discussion

Here an enhancement of the AODV protocol is provided by proving more security after detecting the single or

Table 1 Simulation Parameters

Parameter	Value
Terrain Area	800 m x 800 m
Simulation Time	50 s
MAC Type	802.11
Application Traffic	CBR
Routing Protocol	AODV
Data Payload	512 Bytes/Packet
Pause Time	2.0 s
Number of Nodes	15
Number of Sources	1
No. of Adversaries	1 to 3

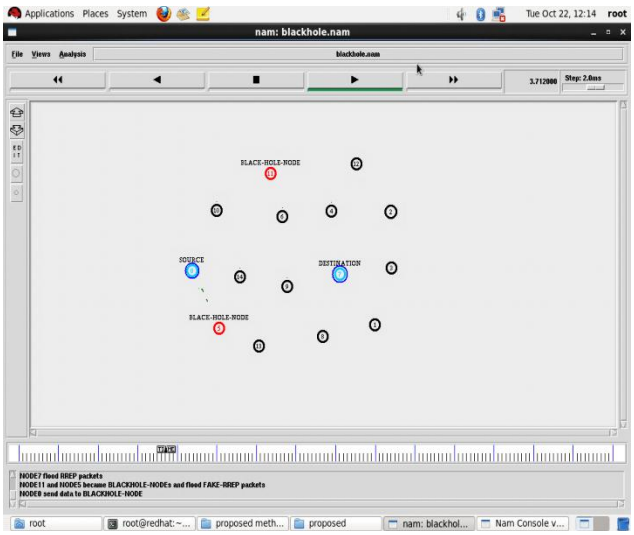

Fig. 3: Black hole node dropping packets

black hole nodes in MANET. 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. The proposed scheme does not alter the standard AODV protocol but acts as an enhancement to isolate black hole nodes before the actual route discovery process starts. This introduce an extra work of sending fake RREQ to the nodes and then checking the replies and isolating the malicious nodes. But this extra work can save the network from the degradation of performance.

The figure 4 shows the gain in throughput when the proposed scheme is used before the actual route discovery process. Throughput increases as more and more packets are delivered to the destination as against the standard AODV protocol where the throughput decreases due to the presence of the black hole nodes in the network.

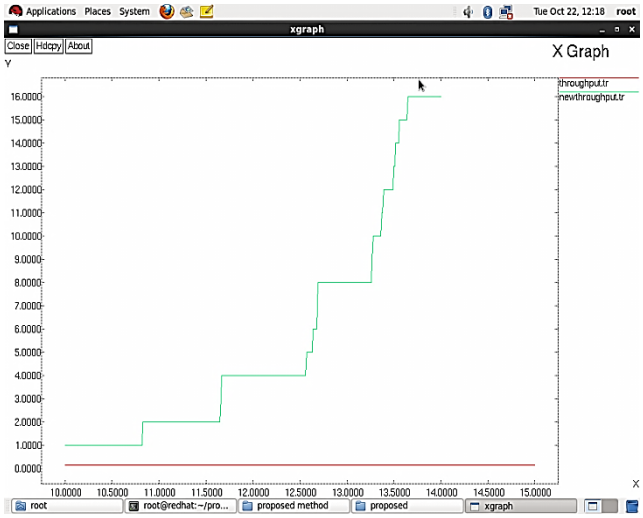

Fig. 4: Graph for increased throughput

The figure 5 shows the minimum delay while using the proposed method. Whereas the delay continues to increase in the presence of the black hole node in case of standard AODV routing protocol.

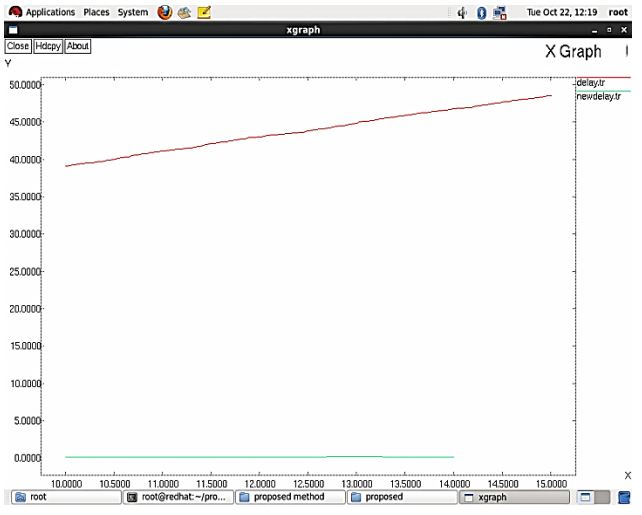

Fig. 5: Decreased end-to-end delay

The parameters like PDR, end to end delay are used for checking if packets are dropped again or not, so that again detection can be done. So, whenever there is change in PDR and end to end delay as compared to average PDR and average end to end delay, there is need to detect the malicious node. The proposed scheme has been implemented using network simulator (NS2). Also testing of the new scheme against parameters like throughput and end-to-end delay has been done.

References

M. Medadian, M. Yektaie and A. Rahmani (2009), Combat with Black Hole Attack in AODV Routing Protocol in MANET, *IEEE.*

S. Lu, L. Li, K.-Y. Lam and L. Jia (2009), SAODV: A MANET Routing Protocol that can withstand Black Hole Attack, *IEEE*, pp. 421-425.

J. Sen, S. Koilakinda and A. Ukil (2011), 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.

P. K. Singh and G. Sharma (2012), An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET, *IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 902-906.

N. Sharma and A. Sharma (2012), The Black Hole node attack in MANET, *IEEE Second International Conference on Advanced Computing & Communication Technologies*, pp. 546-550.

M. Patel and S. Sharma (2013), Detection of Malicious Attack in MANET: A Behavioural Approach, *IEEE International Advance Computing Conference*, pp. 388-393.

M. Jhansi, K. R. Devi and B. M. Chandra (2012), Effective Measure to prevent Cooperative Black Hole attack in Mobile Ad-hoc Wireless Networks, *International Journal of Engineering Research and Applications, vol. 2, no. 4, pp. 204-209.*

Rutvij H. Jhaveri (2013), MR-AODV: A Solution to mitigate Black hole and Gray hole attacks in AODV based MANET's, *Internation Conference on Advanced Computing & Communication Technologies*, pp. 254-260.