MAT JOURNALS

Journal of VLSI Design and Signal Processing
Volume 3 Issue 1

Performance Comparison of ZHLP and M-ZHLP under Black Hole for Manet

K. Thamizhmaran
Department of Electronics and Communication Engineering,
Annamalai University, Annamalai Nagar,
Chidambaram, Tamilnadu, India-608002
E-mail: tamil5_happy@yahoo.co.in

Abstract

Mobile Ad-hoc Networks (MANETs) are a type of Wireless ad-hoc network that usually has a routable networking environment on top of an end-to-end Link Layer (LL) ad-hoc network. MANETs consist of a hop-to-hop, self-arrangement and self-configure network in contrast to a mobile network has a central controller. The solutions may not always be sufficient, as ad-hoc networks have their own vulnerabilities that cannot be addressed by these IDS solutions. In the network, some active attacks un-forward capacity nodes pretend to be intermediate nodes of a route to some given targets, drop any packet that subsequently goes through it, is one of the main types of attack. In this research paper, they propose black-hole attacks an analysis method to detect malicious nodes in MANETs, the mechanism is cooperative hence the protocol work cooperatively together so that they can analyze, detect malicious nodes in a reliable manner. To verify our developed scheme by running through Network Simulations 2 (NS2) with mobile nodes using hybrid routing protocol namely, Modified - Zone based Hierarchical Link State (M-ZHLS) routing protocol. It is observed that the black hole and malicious node detection rate is very good, reduced average delay and also increased packet delivery ratio compare Zone based Hierarchical Link State (ZHLS) routing protocol when there is a change of mobility speed and varying topology size.

Keywords: *Ad-hoc network, Mobile ad-hoc network, Attacks, Black hole, M-ZHLP, PDR, Overhead, Throughput.*

INTRODUCTION

A mobility nature of MANETs may be a collection of every self-employed mobile node with in efficient network which will communicate to all various mounted through radio waves. The mobile nodes that area unit in radio vary of every different will communicate directly, whereas others want the help of intermediate nodes to route their packets. Each node encompasses a through air interface to speak with different nodes. These networks area unit absolutely distributed, and may work anyplace while not the assistance of any mounted infrastructure as access points or base stations. It lacks centralized administration and is connected by wireless links or cables. Wireless ad hoc network can be build up where there is no support of wireless access or wired backbone is not feasible [1]. Black hole problem in MANETS is a serious security problem to be solved in this problem; a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. In flooding based protocol, if the malicious reply reaches the requesting node before the reply from the actual node, a forged route has been created. This malicious node then can choose whether to drop the packets to perform a denial-of-service attack or to use its place on the route as the first step in a man-in-the-middle attack. Unplanned network area unit in the main subjected to 2 totally different levels of attacks [2]. The primary level of attack happens on the fundamental mechanisms of the unplanned network

love routing. Whereas the second level of attacks tries to break the safety mechanisms utilized within the network. Hence the performance compares the increase in malicious nodes.

ATTACK

The threats on a MANET can be from the un-authorized intermediate nodes those are outside are inside the network of nodes. Threats from the nodes external of the network are likely to be detected easily than the internal nodes of the network, in MANET can be broadly divided into 2 categories such as external threats and internal threats. In this research paper, detect one of the internal attack block-hole attacks from source to destination [3, 4].

Black Hole Attack

In this type of attacks, malicious node claims having an optimum route to the node whose packets it wants to intercept. On receiving the request the malicious node sends a fake reply with extremely short route. Once the node has been able to place itself between the communicating nodes, it is able to do anything with the packets passing between them. In Figure 1, malicious node "4" advertises itself in such a way that it has a shortest route to the destination. When source node "S" wants to send data to destination node "D", it initiates the route discovery process. The malicious node "4" when receives the route request, it immediately sends response to source. If reply from node "4" reaches first to the source than the source node "S" Ignores all other reply messages and begin to send packet via route node "2". As a result, all data packets are consumed or lost at malicious node.

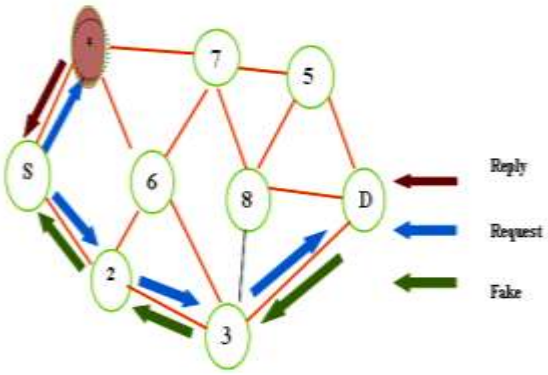

Fig. 1: *Black Hole Attack.*

BACKGROUND

A weighted clustering algorithm for mobile ad-hoc networks was highlighted by Chatterjee, *et al.* (2002). A survey of clustering schemes for mobile ad hoc networks was done by Jane Yu, Peter Chong (2005). A simple clustering mechanism for OLSR Challenges in ad-hoc networking was discussed by Baccelli (2006). A cluster-based OLSR extension to reduce control overhead in mobile Ad hoc networks was taken by Ros FJ, Ruiz PM (2007). Mobile computing was taken by Imielinski, *et al*. (2010). Performance comparison of routing protocol in MANET was analyzed by Prabu, *et al.* (2012). A survey routing protocols in MANET was specified by Swati, *et al.* (2014). An improved cluster maintenance scheme for mobile Adhoc networks was analysed by Pathak, *et al.* (2014) [5, 6].

PROPOSED METHOD

To detect the malicious node we have proposed two methods which use a hybrid routing protocol known as existing Zone based Hierarchical Link State (ZHLS) routing protocol and Modified-Zone based Hierarchical Link State (M-ZHLS) routing protocol for analysis of the under effect of the black-hole attack when the destination sequence number is changed via NS2.

DESIGN OF M-ZHLS

Modified - Zone based Hierarchical Link State (M-ZHLS) routing protocol like

hybrid routing protocol, is that topology information is only transmitted by nodes on-demand.

RREQ - As an optimization M-ZHLS uses an expanding ring technique when flooding these messages. Every RREQ carries a time to live (TTL) value that states for how many hops this message should be forwarded.

RREP - RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address.

RERR - When a link breakage in an active route is detected, a RERR message is used to notify other nodes of the loss of the link.

Node 1 after receiving the further detection message broadcast a RREQ message by setting destination address to source nodes address. If it receives a RREP message from the malicious node, it sends a Test packet (TP) to the source node via malicious node, and at the same time it sends an Acknowledgment Packet (AP) to Source Node (SN) though some other route [7, 8].

S 1. Source node broadcast RREQ packet along with the destination ID
S 2. For every intermediate receives the RREQ check
S 3. For every node IN receives RREP Check
S 4. After receiving the reply, source node broadcast a FD message to all mobile nodes
S 5. For every mobile node receive further detection message
S 6. Source node waits for „wt‟ time
S 7. If all the flags are „N‟,
S 8. End.

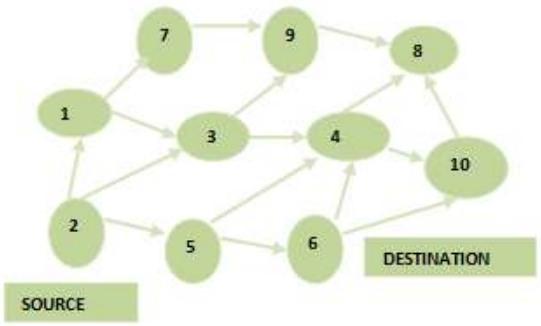

Fig. 2: *Simple Mobile Ad-hoc Network 10 Nodes.*

As in Figure 2, source is node 1 and the target is node 10. If we consider node 6, first it will find out the nodes which are within its radio range and store in its N-List. According to Figure 1 neighbor list of node 6 are 3, 4, 5, 8 and 9. Then node 6 sends the RREQ to all its neighbor nodes each neighbor node that receives the broadcast checks the destination to see if it is the intended recipient. If yes it sends a RREP message back to the node 6. RREP message contains the current sequence number of the destination node. At the same time node 3, 4, 5, 8, 9 maintain the sequence number in the source node time and sequence numbers are generated randomly.

SIMULATION CONFIGURATION

Our experiments via network simulator 2.34, a scalable simulation environment for network systems; the routing protocol we use is M-ZHLS comparing the simulation results with other research works. The maximum hops allowed in this configuration setting, in Table 1 simulation parameters are given below.

Table 1: *Simulation Parameter.*

Parameter:	**Value**
Simulation area	800 m * 800 m
Number of nodes	25,50,75,100,125,150
Average speed of nodes	0–20 meter/second
Mobility model	Random waypoint
Number of packet per/sec	6
Transmission range	100 m
Constant bit rate	4 (packets/second)

Packet size	512 bytes
MAC protocol	802.11 DCF
Initial energy/node	100 joules
Antenna model	Omni directional
Simulation time	1000 sec

Performance Evaluation

Our research work, simulated network consists of nodes like, 25, 50, 75, 100, 125, 150 mobile nodes placed randomly within fixed topology size. All nodes have the same transmission range of 100 meters the channel capacity is 2.5 Mbps. The random waypoint model was used in the simulation runs. In this model, a node selects a destination randomly within the roaming area and moves towards that destination at a predefined speed 30 m/s. our results analysis the following parameters packet delivery ratio, routing overhead and throughput.

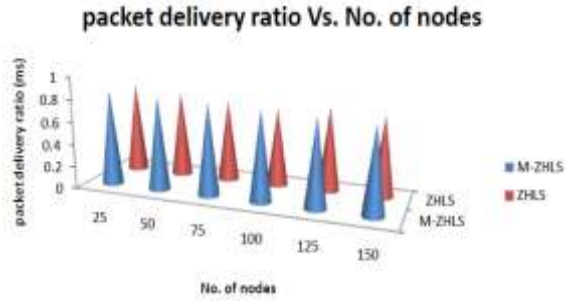

Fig. 3: *Packet Delivery Ratio vs. Number of Nodes.*

From Figure 3 it is clear that our suggested scheme M-ZHLS surpassed ZHLS performance by above 4% when there are 1 to 150 of nodes in the network. M-ZHLS is able to detect malicious nodes in the presence of block-hole attacks.

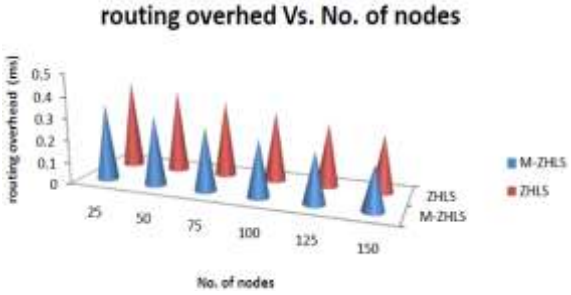

Fig. 4: *Routing Overhead vs. Number of Nodes.*

Figure 4 clearly depict comparison of M-ZHLS with corresponding internal attack algorithm along with M-ZHLS where it shows the routing overhead deceases with increase in the number of nodes on by 1 to 150.

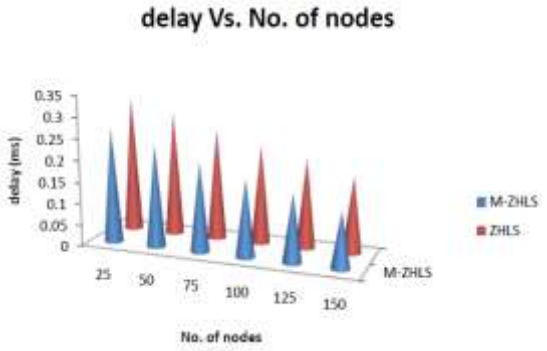

Fig. 5: *Delay vs. Number of Nodes.*

According to Figure 5, it is clear that in all, the proposed scheme M-ZHLS surpassed the performance of ZHLS in minimising delay by 5% when there are 1 to 150 nodes in the network. As the developed scheme finds various maximum forward capability nodes in primary stage, it is possible to minimize the delay.

CONCLUSION AND FURTURE WORK

In this paper, a Black hole attack is one of the most important security problems in MANET. The proposed algorithm is a black hole attack causes dropping of data packets by malicious nodes in the path source to destination. This M-ZHLS provides better performance compared to the existing ZHLS routing protocol by decreasing average delay by 5% lowering routing overhead by 4% and increase delivery ratio by 4.5%. This approach reduces the chances of unnecessary topology; the algorithm of M-ZHLS is simulated in ns-2 and compared with

ZHLS protocol. In future work is to implement the hybrid network with minimum delay and higher throughput and also test real time environment.

REFERENCES

1. Chatterjee, et.al (2002) "A Weighted Clustering Algorithm for Mobile Ad Hoc Networks", Vol. 5, No. 2, pp. 193-204.
2. Jane et al, (2005) "A Survey of clustering schemes for MANET", *IEEE communication and surveys*, Vol.7, No.1, pp. 32-47.
3. Baccelli (2006) "OLSR trees: A simple clustering mechanism for OLSR", *International Federation for Information Processing*, Vol. 197, pp. 265–274.
4. Ros FJ and Ruiz PM (2007) "Cluster-based OLSR extensions to reduce control overhead in mobile Ad hoc networks", *In Proc. of the conference on WC & MC-ACM*, New York, pp. 202–207.
5. Imielinski, et al (2010) "Mobile Computing", *Springer publications*, Vol. 76, No. 12, pp. 1281-1293.
6. Prabu, et al (2012) "Performance Comparison of Routing Protocol in MANET", *IJARCSSE*, Vol-2, No. 9, pp. 388-392.
7. Swati, et.al (2014) "A Survey Routing Protocols in MANET", *IJCA*, Vol. 96, No. 13, pp. 7-12.
8. Pathak, et al (2014) "An improved cluster maintenance scheme for MANET", *In IEEE Conference on advances in computing, communications and informatics*, pp. 2117–2121.