Performance Evaluation of FSR, DYMO and LANMAR Routing Protocols

Satveer Kaur [1]
Research Scholar [1]
CT Group of Institutions, Jalandhar.

Shivani Khurana [2]
Assistant Professor[2]
CT Group of Institutions, Jalandhar

ABSTRACT

Mobile Ad hoc Network (MANET) is a collection of mobile nodes that are arbitrarily located so that the interconnections between nodes are energetically altering [1]. In MANET mobile nodes forms a temporary network without the use of any existing network infrastructure or centralized administration. A routing procedure is used to find routes between mobile nodes to facilitate communication inside the set of connections. The main goal of such an ad hoc network routing protocol is to establish correct and efficient route between a pair of mobile nodes so that messages delivered within the active route break intermission. Route should be discovered and maintained with a minimum of overhead and bandwidth expenditure. This article presents performance evaluation of three different routing protocols i.e. Fisheye Source Routing (FSR), Landmark Adhoc routing protocol (LANMAR), and Dynamic MANET on Demand Routing Protocol (DYMO) with respect to different nodes. Performance of FSR, LANMAR and DYMO is evaluated based on Throughput and Average end to end delay with and without Black hole Attack.

Keywords

Adhoc networks, FSR, DYMO and LANMAR, Black Hole Attack.

1. INTRODUCTION

Mobile Ad Hoc Networks are the self-organizing and self-configuring wireless networks which do not rely on a fixed infrastructure and have the capability of rapid deployment in response to application needs. Nodes of these network function as routers which discover and maintain routes to other nodes in the network. Ad-hoc networks were first mainly used for military applications. Since then, they have become all the time more popular within the computing industry. Applications include casual conference, meeting, fundamental classrooms, emergency search-and-rescue operation, disaster respite operation, automated battleground and operations in environments where construction of infrastructure is difficult or expensive [2]. In MANETs, due to lack of centralized entity and the mobile nature of nodes, network topology changes frequently and changeably. Hence the routing protocols for ad hoc wireless networks have to adapt quickly to the frequent and impulsive changes of topology [11]. There are many routing protocols available for Ad-hoc networks such as AODV, CGSR, DSDV, DSR, DYMO, FSR, GSR, OLSR, STAR, TORA, WRP and ZRP etc. In this paper we study three routing protocols: FSR, LANMAR and DYMO and evaluated the performance of these three routing protocol l under black hole attack: In Section 1 it describes introduction, 2nd section includes simulation setup and in 3rd section it includes conclusion.

A. FISHEYE STATE ROUTING (FSR)

Fisheye State Routing (FSR) protocol is a proactive (table driven) ad hoc routing protocol and its mechanisms are based on the Link State Routing protocol used in wired networks. FSR is an understood hierarchical routing protocol. It reduces the direction-finding update overhead in large networks by using a fisheye technique [3]. Fish eye has the ability to see the objects better when they are nearer to its focal point that means each node maintains accurate information about near nodes and not so accurate about far-away nodes. The range of fisheye is defined as the set of nodes that can be reached within a given number of hops. Fig. 1 shows the scope of fisheye. The number of levels and the radius of each scope will depend on the size of the network. Entries equivalent to nodes within the smaller scope are propagated to the neighbors with the highest frequency and the exchanges in smaller scopes are more frequent than in larger. That makes the topology in sequence about near nodes more precise than the information about farther nodes [10]. FSR minimized the consumed bandwidth as the link state update packets that are exchanged only among neighboring nodes and it manages to reduce the message size of the topology information due to removal of topology information concerned far-away nodes. Even if a node doesn't have precise in sequence about far missing nodes, the packets will be running scared correctly because the route information becomes more and more accurate as the packet gets closer to the destination. This means that FSR balance well to large mobile ad hoc networks as the overhead is controlled and supports high rates of mobility [12]. The FSR concept originates from Global State Routing (GSR). GSR can be viewed as a special case of FSR, in which there is barely one fisheye scope level and the radius is infinite. As a result, the entire topology table is exchanged among neighbors that consume a considerable amount of bandwidth when network size becomes large.

B. DYMO

The Dynamic MANET On-demand (DYMO) is a reactive, multihop, unicast routing protocol [9]. The DYMO is a recollection concerned routing protocol and stores minimal routing information and so the Control Packets is generated when a node receives the data packet and it doesn't have any valid route information. The essential operations of DYMO are:

A. Route Discovery

B. Route Maintenance

Route Discovery

The source router generates Route Request (RREQ) messages and floods them for destination routers for whom it doesn't have route information [5]. In-between nodes store a route to the originating router by adding it into its routing table during this dissemination process. The target node after receiving the RREQ responds by sending Route Reply (RREP) message.

RREP is sent by uncast technique towards the source. A middle node that receives the RREP creates a route to the target and so finally it reaches to originator. Then routes have been traditional between source and destination in both directions.

Route Maintenance

Route maintenance consists of two operations. It avoids failing good routes and so it updates reverse route lifetime on data reception and forward route lifetime on data transmission. The DYMO node monitors association over which traffic is flowing in order to cope up with dynamic network topology. A Route Error (RERR) message is generated when a node receives a data packet for the destination for which route is not known or the route is broken. This RERR notifies other nodes about the link failure. The basis node reinitiates route detection quickly as it receives this RERR. Hello communications are used by all nodes to maintain routes to its neighbor nodes The sequence numbers are used in DYMO to make it loop free. These sequence numbers are used by nodes to determine the order of route discovery messages and so avoid propagating stale route information. The DYMO routing protocol is designed for memory constrained devices in mobile ad hoc networks (MANETs) as it quickly determines route information dynamically.

C. LANMAR

LANMAR is an effective proactive based routing protocol which uses the same approach of Fisheye State Routing (FSR).Routing table and Node distance is evaluated using hop counts in the given network topology. LANMAR provisions a exact address each node reflects its position within the hierarchy and enables LANMAR to discover and maintain a specific route. All the nodes in a specific chain of command region gain knowledge of route to communicate with each other. Moreover, each node will be defined with a specific "landmarks" at different hierarchical levels [6]. In LANMAR routing protocol there is consistent packet forwarding and the path is redefined from top level hierarchy to lower level hierarchy [13]. When a node requires sending a packet within its hierarchical province, the route information is identified from the routing table stored within the hierarchical region. Otherwise, node evaluates the rational subnet field of the destination and the packet is forwarded towards the landmark for that consistent subnet [7]. Topological changes and route information will be updated periodically within the hierarchical nodes with one hop distance. In each revise the nodes will send the route information based on its fisheye scope. By this update procedure, the routing entries with larger sequence information are replaced with smaller sequence information.

2. SIMULATION SETUP

QualNet 5.0 Network Simulator tool is used to evaluate the performance of different Ad hoc routing in Wireless sensor networks. In this simulation, we have tested routing protocols with 15, 20, 25, 30, 50 nodes [4]. The nodes are deployed randomly. CBR is used as data traffic application with multiple source and destination.

Random Waypoint Mobility Model

In this model, the node selects a random location, moves towards it in a in a straight line line at a constant speed that is randomly selected from a range, and pause at that target. The node repeats this, right through the simulation [14]. To evaluate the performance of routing protocols, we used two different quantitative metrics to compare the performance of FSR, LANMAR and DYMO routing protocol. They are Average end to end delay and Throughput. The parameters used in the simulation are summarized in the table below.

Table 1. Simulation Parameters

Parameters	Values
Routing Protocols	802.11
MAC Layer	512 Bytes
Packet Size	512 Bytes
Terrain Size	1500*1500
Nodes	15,20,25,30,50,70
Mobility Model	Random Waypoint Model
Data Traffic Rate	CBR
No. of Source	5
Simulation duration	30 sec
CBR Traffic Rate	8 packet/sec
Attack Type	Black hole Attack

2.1 Performance metrics

Performance Metrics used to calculate the performance are:

a. Average End to End Delay

End-to-end delay indicates how long a packet takes to travel from the CBR source to the application layer of the destination. This includes all probable delays caused by buffering during route discovery latency propagation and transfer times.

b. Throughput

The Throughput is defined as the total amount of data a receiver receives from the sender divided by the time it takes for the receiver to get the last packet [8]. The throughput is considered in bits per second (bit/s or bps).

Case 1. Performance evaluation of FSR Routing protocol in terms of Throughput and Average end to end delay with and without black hole attack

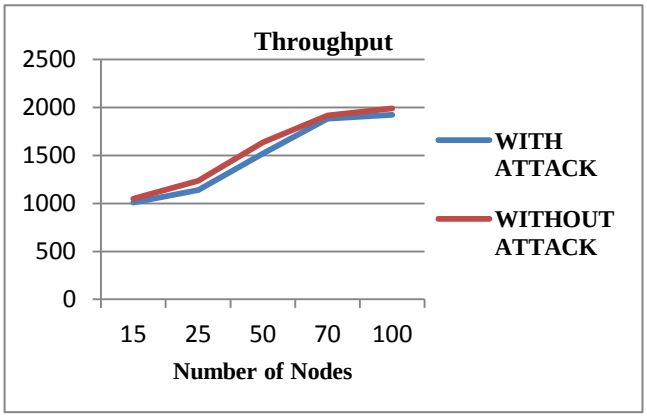

Fig 1 . Throughput

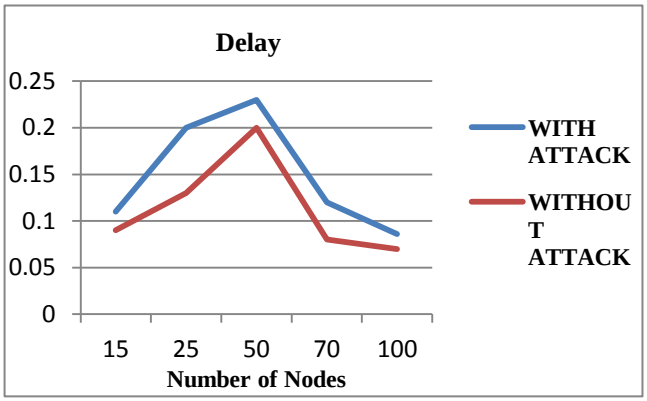

Fig 2. Average end to end delay

Case 2. Performance evaluation of LANMAR Routing protocol in terms of Throughput and Average end to end delay with and without black hole attack

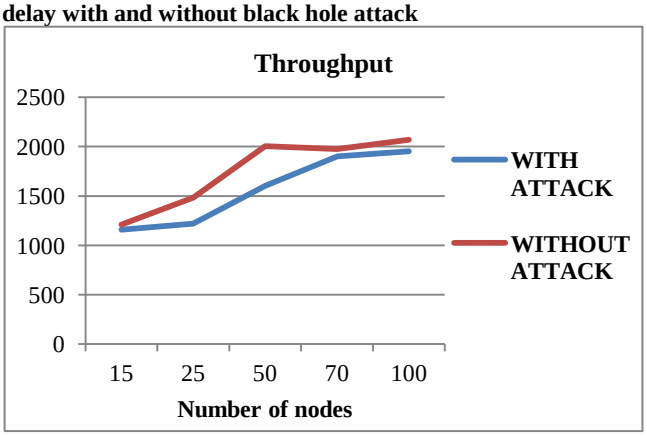

Fig 3. Throughput

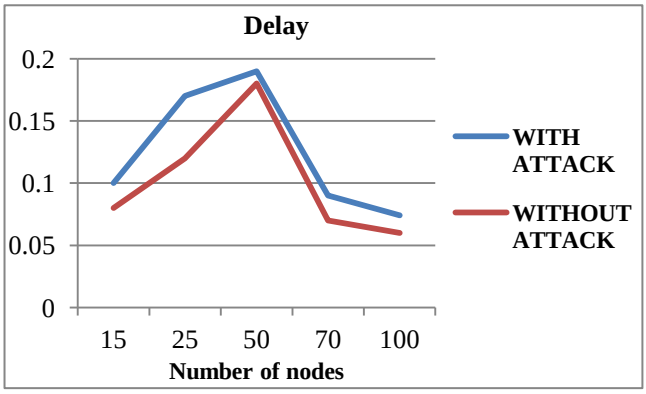

Fig 4. Average end to end delay

Case 3. Performance evaluation of DYMO Routing protocol in terms of Throughput and Average end to end delay with and without black hole attack

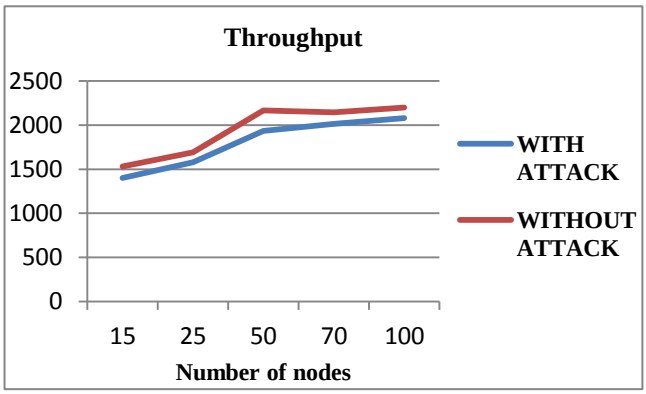

Fig 5 .Throughput

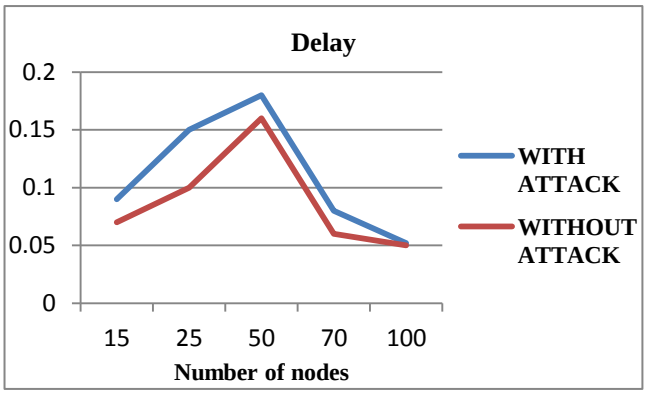

Fig 6 . Average end to end delay

3. CONCLUSIONS

The Performance of these routing protocols is evaluated with respect to two performance metrics such as Average end to end delay, Throughput. According to our simulation results, DYMO shows best performance than LANMAR and FSR in terms of throughput and Average end to end delay. So it observes that black hole attack decrease the performance of routing protocols because these malicious nodes drop the data packets. We plan to extend my work on the black hole

detection and prevention scheme using some kind of security algorithm.

4. REFERENCES

[1] Anuj Gupta, Navjot Kaur, Amandeep Kaur "A Survey on Behavior of AODV and OLSR Routing Protocols of Manets under Black Hole Attack" IJCST Vol. 2, Issue 4, Oct . Dec. 2011.

[2].Surbhi Sharma, Himanshu Sharma "Performance Comparison of AODV, DSR, DYMO and ANODR using QualNet Simulator" International Journal of Computer Information Systems, Vol. 2, No. 6, 2011.

[3] Parma Nand, Dr. S.C. Sharma "Traffic Load based Performance Analysis of DSR, STAR & AODV Adhoc Routing Protocol" IJCST Oct. - Dec. 2011.

[4] R. Parthasarathy, A. PravinRenold "Performance Analysis of OLSR, AODV and ZRP with Fault in Mobile Ad Hoc Networks" International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012.

[5] Yih-Chun Hu, Adrian Perrig, David B. Johnson " Black hole Attacks in Wireless Networks" IEEE Journal on Selected Areas In Communications" Vol. 24, No. 2, pp370-380,Feb 2006.

[6] G. Pei, M. Gerla, X. Hong, and C.-C. Chiang, "A Wireless Hierarchical Routing Protocol with Group Mobility," In IEEE WCNC'99, New Orleans, LA, Sep. 1999, pp.1536-1540.

[7] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Worm hole Attacks in Wireless Networks" IEEE Journal on Selected Areas In Communications,Vol. 24, No. 2, pp370-380,Feb 2006.and System Modeling, 2010.

[8] Rashid Sheikh, Mahakal Singh Chandel, durgesh Kumar Mishra. "Security issues in MANET: A Review" IEEE, 2010.

[9]. E.D. Kaplan (Editor) "Understanding the GPS: Principles and Applications, Artech House, Boston, MA" Feb. 1996.

[10] L. Klein rock and K9 "Fahim Maan, Nauman Mazhar. MANET Routing Protocols vs. Mobility Models: A Performance Evaluation" ICUFN, 2010.

[11] MIAO Quan-xing, XU Lei. "DYMO Routing Protocol Research and Simulation Based on NS2 International Conference on Computer Application. Stevens, "Fisheye: A Lenslike Computer Display Transformation," Technical report, UCLA, Computer Science Department 2010.

[12] Fahim Maan, Nauman Mazhar "MANET Routing Protocols vs. Mobility Models: A Performance Evaluation," CUFN, 2012.

[13] MIAO Quan-xing, XU Lei "DYMO Routing Protocol Research and Simulation Based on QUALNET" International Conference on Computer Application and System Modeling, 2011.

[14] Rashid Sheikh, Mahakal Singh Chandel, durgesh Kumar Mishra "Security issues in MANET: A Review" IEEE, 2010.