ISSN:0975-9646

Performance Evaluation of FSR, DYMO & LANMAR Routing Protocols under Blackhole Attack

Satveer Kaur [1] Shivani Khurana [2]

Research Scholar [1] Assistant Professor[2]
CT Group of Institutions,
Jalandhar.

Abstract: The Wireless adhoc network is comprised of nodes with wireless radio boundary. Nodes are joined among themselves and are free to move. It is a multi hop process due to the incomplete transmission range of energy constrained wireless nodes. Many protocols are reported in this field but it is difficult to decide which one is best. In this paper FSR, DYMO and LANMAR are surveyed and characteristic summary of these routing protocols is presented under Blackhole Attack. Their performance is analyzed on packet delivery ratio, Throughput, Average end to end and Jitter using Qualnet 5.1 simulator.

Keywords: **Adhoc networks, FSR, DYMO and LANMAR, Performance.**

1. INTRODUCTION

Mobile Ad-Hoc Network is a group of wireless mobile nodes associated to each-other without any inner administrator. The nodes can leave or bond the network at any time. Due to the movement of nodes the topology of the network changes rapidly. The nodes which are close to every other or within each other's radio range can attach directly. But nodes which are far away they use middle nodes to send data. MANETs has benefits like they are Simple, cheap and fast networks. The confront in MANETs is equipping any devices to continuously maintain the information required to properly route traffic. Wireless networking is an emerging technology that allows users to access information and services by electronic means, regardless of their geographic location. Wireless networks can be classified in two types.

Infrastructure Networks

Infrastructure network consists of a set of connections with fixed and agitated gateways. A mobile host communicates with a viaduct in the network (called support station) within its communication radius. The mobile unit can move biologically. When it goes out of array from one base station, it connects with new support station and starts communicating from side to side it. This is called handoff. In this approach the base station are fixed.

Infrastructure less (Ad hoc) Networks

In ad hoc network all nodes are mobile and can be coupled with passion in an illogical manner. As the array of each host's wireless transmission is limited, so to converse with hosts exterior its broadcast range, a host needs to join the aid of its nearby hosts which forward packets to the destination. So all nodes of this network behave as routers and take part in discovery and conservation of routes to other nodes in the network. Ad hoc Networks are very helpful in crisis search-and rescue operations, meetings or convention in which\ persons wish to quickly share information, and data acquisition operations in inhospitable terrain. These informal routing protocols can be divided into two categories

Table-Driven Routing Protocols: In table driven routing Protocols, dependable and up-to-date routing information to all nodes is maintained at each n ode.

On-Demand Routing Protocols: In On-Demand routing Protocols, the routes are shaped as and when required. When a source wants to propel to a purpose, it invoke the route discovery mechanism to find the path to the purpose.

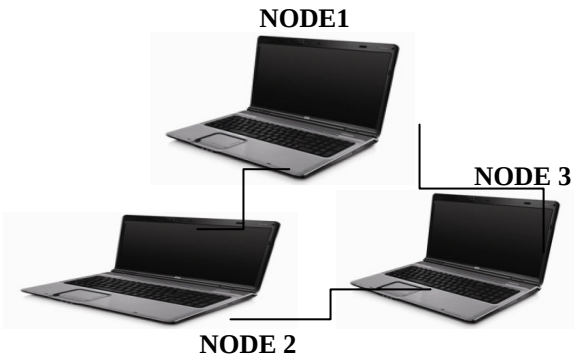
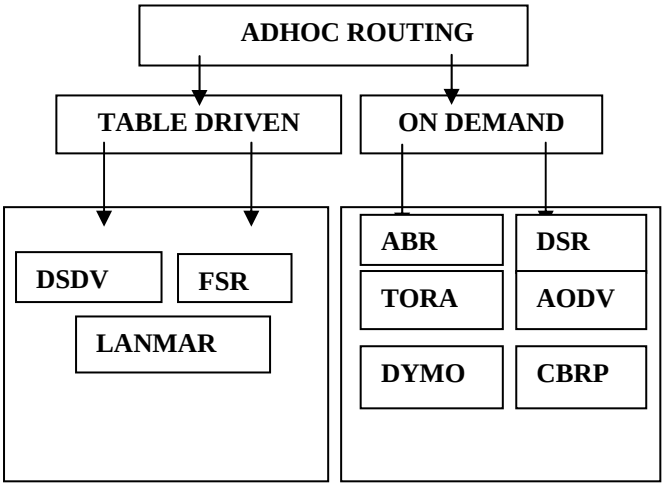


Fig1. MANETS

2. ROUTING PROTOCOLS

Proactive protocols are also known as table determined protocols. In proactive protocols nodes preserve a route in own routing tables to all the target nodes in the network. For this routes are discovered for every mobile node of the network, without any request for communication by the hosts. Some of proactive protocols are FSR, DSDV, OLSR, ANODR and STAR. Reactive protocols are also known as on-demand routing protocols shown in fig 2. In these protocols a route is only discovered when source node want to send data to the destination node. Some of the reactive routing protocols are DSR, AODV and DYMO. Due to the arbitrary movement of nodes, the topology becomes changeable and changes rapidly. In order to find the most adaptive and efficient routing protocols for dynamic MANET topologies, the Routing protocols need to be analyze at node speeds, network size, network mobility ,number of transfer and node density. LANMAR, FSR and DYMO routing protocols are used in simulation.



2.1 Fisheye State Routing (FSR)

FSR is an implicit hierarchical routing protocol. It uses the "fisheye" technique proposed by Klein rock and Stevens, where the technique was used to reduce the size of information required to represent graphical data. The eye of a fish captures more detail pixels near the focal point. The detail relegate as the distance from the focal point increment. In routing scheme, this approach translates to maintain accurate distance and path quality information about the neighborhood of a node. FSR is a hierarchical routing protocol. It maintains the topology of the network at every node but does not flood the entire network with information. Instead of flooding, node exchanges topology information only with its neighbors. Recent topology changes are identified using sequence numbers

2.2 DYMO

It is a successor of AODV. It is a combination of AODV and DSR routing protocols. Similar to AODV, DYMO has two main operations, route discovery and route preservation. In route discovery, the sender node broadcast a RREQ message all through the network to find the destination node. During this process, each in among nodes records a route to the source node and rebroadcast the RREQ after appending its own address. This is called the path a accretion function. When the destination node receives the RREQ, it responds with RREP to the resource node. Each intermediate node that receives the RREP records a route to the purpose node. When the source node receives RREP message, the route is established between the source node and the destination node. As path buildup function can reduce the route overhead, and the small package size of the routing packet is increased. When a link break, the source of the packet is notified RERR message is send to the sender node like acknowledgement.

2.3 LANMAR

Landmark ad hoc routing protocol (LANMAR) The Landmark Ad-hoc Routing Protocol (LANMAR) is designed to dramatically reduce routing table size and routing update overhead in large-scale ad-hoc networks that exhibit group mobility. LANMAR same as the features of (FSR) and; this added some features like landmark election to cope with the dynamic and mobile environment. Other benefits of LANMAR include the uses of landmark for each logical group in order to reduce routing update overhead, and the exchange of "scoped" link state with neighbors only. By virtue of land marking, remote groups of nodes are "summarized by the corresponding landmarks. As a result, each node still maintains accurate routing information about immediate neighborhood; at the same time it will keep track of the routing directions to the landmarks nodes, and thus, to remote group

3. SECURITY IN MANETS:

A lot of research was done in the past but the most significant contributions were the PGP (Pretty first-class Privacy) and the trust based security but none of the protocols made a decent tradeoff between security and performance. In addition to reflect security in MANETs many researchers have suggested and implement new improvements to the protocols and some of them have suggested new protocols. Ad-hoc networks are highly susceptible to security attacks and dealing with this is one of the main challenges of developers of these networks today. The main reason for this complicatedness are; Shared non secure operating environment, lack of central power, lack of organization among nodes, less availability of resources, and physical weakness.

Classification of attacks on MANETs:

These attacks on MANETs confront the mobile infrastructure in which nodes can join and leave easily with dynamics requests without a static path of direction-finding. Schematics of various attacks as described below:

- Application Layer: cruel code, denial of examination
- Transport Layer: Assembly Hijacking, Flooding
- Network Layer: Sybil, flood, Black Hole, Grey Hole. Worm Hole, Link Spoofing, Link preservation, Location revelation etc.
- Data Link/MAC: Unbearable Behavior, Self-Centered Behavior, Active, Passive, Inner outside
- Physical: Interfering, Traffic congestion, Eavesdropping

In this paper the comparison of FSR, DYMO and LANMAR with wormhole is analyzed and presented under Blackhole Attack This paper will explores the impact of packet delivery ratio, Throughput, Average end to end delay and Jitter.

3.1 Blackhole Attack

In a black hole attack, malicious nodes sends fake routing information, claiming that it has a finest route and cause other good nodes to route data packets through the malicious one. The blackhole attack has two properties. earliest, the node exploit the mobile ad hoc routing procedure ,to advertise itself as having a valid route to a purpose node, even although the route is false, with the meaning of intercepting packets. Second, the assailant consumes the intercepted packets without any forwarding. However, the attacker runs the danger that neighboring nodes will monitor and expose the ongoing attacks. There is a more subtle form of these attacks when an assailant selectively forwards packets. An attacker suppress or modifies packets originating from some nodes, while send-off the data from the other nodes..

4. RELATED WORK

The performance of LANMAR, DYMO and FSR protocols were evaluated with respect to parameters such as packet delivery ratio, throughput, average jitter and end-to-end delay with a mobile and immobile network with Blackhole Attack using Qualnet 5.1

Table 1. Performance Metrics

Throughput	The overall capacity of any system to process its inputs and generate the required output is called the system's Throughput
Packet delivery ratio	It is the ratio that illustrates the total amount of packets delivered to the destination.
Average End-to-End Delay	Average end-to-end delay is the average time it takes a data packet to reach to destination in seconds. It is calculated by subtracting "time at which first packet was transmitted by source" from "time at which first data packet arrived to destination
Jitter	Jitter is the variation in the time between packets incoming, cause by network blocking, and route changes

FUTURE WORK

In Future, the Performances Evaluation of protocols like LANMAR, FSR and DYMO under BLACKHOLE attack can be evaluated by using different type of parameters and different security mechanism should to prevent routing protocols from the different type of attacks.

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. Kleinrock 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.