Simulation Analysis of STAR, DSR and ZRP in Presence of Misbehaving Nodes in MANET

Amrit Suman,
CS Department
TIT, Bhopal, India
amrit.it@gmail.com

Ashok Kumar Nagar
SOIT, RGPV University
Bhopal, India
aknagoriya@gmail.com

Sweta Jain
SOIT, RGPV University
Bhopal, India
sweta.jain.sj@gmail.com

Praneet Saurav
CS Department,
TIT, Bhopal, India
praneetsaurav@gmail.com

Abstract—**Wireless mobile ad-hoc networks are those networks which has no physical links between the nodes. Due to the mobility of nodes, interference, multipath propagation and path loss there is no fixed topology in this network. Hence some routing protocol is needed to function properly for these networks. Many Routing protocols have been proposed and developed for accomplishing this task. The intent of this paper is to study three ad-hoc routing protocols ZRP, DSR and STAR in the presence of some misbehaving nodes and analyze them. This paper concentrates evaluating the performance of routing protocols when some nodes behave as malicious ones. The performance analysis for above protocol is based on variation in speed of nodes in a network with 50 nodes. All simulation is carried out with QualNet 4.5 network simulator.**

Keywords: Ad Hoc Networks, routing protocol, ZRP, DSR, STAR.

I. Introduction

A mobile ad-hoc network (MANET) [1] [2] [3] is a collection of nodes, which are able to connect on a wireless medium forming an arbitrary and dynamic network. MANET implies that the topology may be dynamic - and that routing of traffic through a multi-hop path is necessary if all nodes are to be able to communicate. A key issue in MANETs is the necessity that the routing protocols must be able to respond rapidly to topological changes in the network. At the same time due to the limited bandwidth available through mobile radio interfaces it is imperative that the amount of control traffic generated by the routing protocols is kept at a minimum. Several protocols have been addressed these problems of routing in mobile ad-hoc networks. These protocols were divided into two classes: depending upon the type of requirement and the available resources, when a node acquires a route to a destination.

Proactive protocols [3] are characterized by all nodes maintaining routes to all destinations in the network at all times. Thus using a proactive protocol a node is immediately able to route (or drop) a packet. Examples of proactive protocols include the “Topology Broadcast based on Reverse-Path Forwarding” routing protocol (TBRPF) [2], the “Optimized Link State Routing Protocol” (OLSR) [9] and the “Source Tree Adaptive Routing” (STAR) [6]. *Hybrid* protocols [3][4] are those protocols which have characteristics of both reactive and proactive. Example of hybrid protocol included “Zone Routing Protocol” (ZRP) [4].

Reactive protocols [3] are characterized by nodes acquiring and maintaining routes ON-demand. In general, when a route to an unknown destination is required by a node, a query is region extraction model provides the much better result any animated scene from natural images.

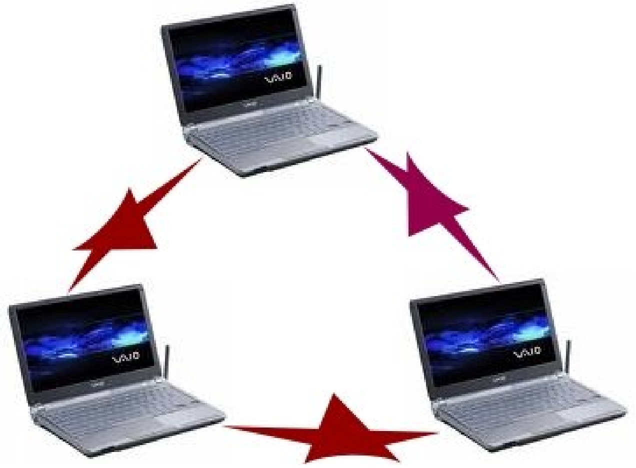


Figure 1:- An example of Ad Hoc Network

Flooded onto the network and replies, containing possible routes to the destination, are returned. Examples of reactive protocols include the “Ad Hoc on Demand Distance Vector Routing Protocol” (AODV) [6] and “Dynamic Source Routing” (DSR) [5].

In this paper, the simulation analysis of three routing protocols (ZRP, DSR, and STAR) is presented. The performance of these protocols is analyzed with varying speed of nodes in network. The network contains 50 wireless nodes in which 10 nodes are misbehaving. These misbehaving nodes either stop packet forwarding or send wrong and unusual information to other nodes which affects packet drop and lesser throughput.

The Organisation of this paper as follows. Section II briefly describes the routing protocols STAR, DSR and ZRP. Section III briefly describes the affects of misbehaving nodes in network. Section IV presents experimental configuration. Section V focused on results and analysis of the work and Section VI represents a conclusion of the paper.

Manuscript received November 15, 2009.

II. ROUTING PROTOCOL

A. STAR (SOURCE TREE ADAPTIVE ROUTING)

The STAR [6][3] protocol is based on the link state algorithm. Each router maintains a source tree, which is a set of links containing the preferred paths to destinations. This protocol has significantly reduced the amount of routing overhead disseminated into the network by using a least overhead routing approach (LORA) to exchange routing information. It also supports optimum routing approach (ORA) if required. This approach eliminated the periodic updating procedure present in the Link State algorithm by making update dissemination conditional. As a result the Link State updates are exchanged only when certain event occurs. Therefore STAR will scale well in large network since it has significantly reduced the bandwidth consumption for the routing updates while at the same time reducing latency by using predetermined routes. However, this protocol may have significant memory and processing overheads in large and highly mobile networks, because each node is required to maintain a partial topology graph of the network (it is determined from the source tree reported by its neighbors), which change frequently may as the neighbors keep reporting different source trees.

B. DSR (DYNAMIC SOURCE ROUTING)

DSR [5] is a fairly simple algorithm based on the concept of *source routing*, in which a sending node must provide the sequence of all nodes through which a packet will travel. Each node maintains its own *route cache* essentially in a routing table. Source nodes determine routes dynamically and only when needed. There are no periodic broadcasts from routers. Figure 2 illustrates the DSR algorithm's route discovery/ route reply cycle. A source node that wants to send a packet first checks its route cache. If there is a valid entry for the destination, the node sends the packet using that route; if no valid route is available in the route cache, the source node initiates the route discovery process by sending a special route request (RREQ) packet to all neighboring nodes. The RREQ propagates through the network, collecting the addresses of all nodes visited, until it reaches the destination node or an intermediate node with a valid route to the destination node. This node in turn initiates the route reply process by sending a special route reply (RREP) packet to the originating node announcing the newly discovered route. The destination node can accomplish this using inverse routing or by initiating the route discovery process backwards. The DSR algorithm also includes a route maintenance feature implemented via a hop-to-hop or end-to-end acknowledgment mechanism; the former includes error checking at each hop, while the latter checks for errors only on the sending and receiving sides. When the host encounters a broken link, it sends a route error (RERR) packet. Dynamic source routing is easy to implement, can work with asymmetric links, and involves no overhead when there are no changes in the network. The protocol can also easily be improved to support multiple routes to the same destination. DSR's main drawback is the large bandwidth

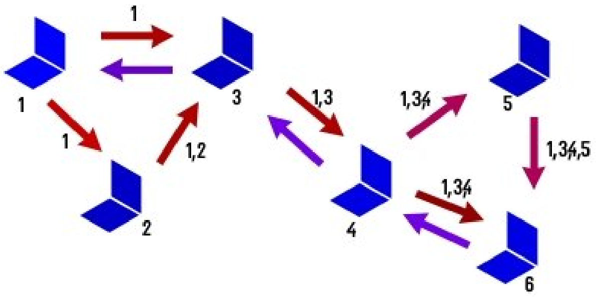


Figure 2:- Dynamic source routing

C. ZRP (ZONE ROUTING PROTOCOL)

ZRP [4] is a hybrid protocols which takes advantage of both table driven and ON-demand routing protocol. In this separation of nodes local neighborhood from the global topology of the entire network allows for applying different approaches and thus taking advantage of each technique's features for a given situation. These local neighborhoods are called *zones* (hence the name) each node may be within multiple overlapping zones, and each zone may be of a different size. The "size" of a zone is not determined by geographical measurement, as one might expect, but is given by a radius of length α where α is the number of hops to the perimeter of the zone.

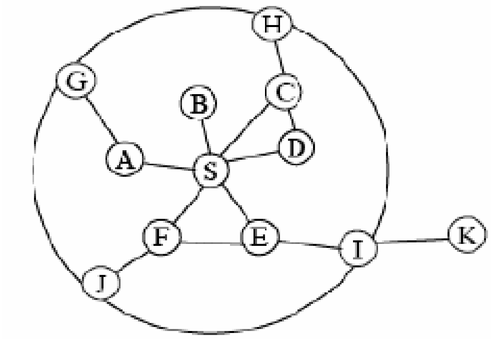


Figure 3:- ZRP

In the above diagram ZRP protocol having Zone radius 2 in this inside the zone communication is done in proactive way and outside it between such zones in reactive way. A, E, F, D are interior node and J, G, I, H are border nodes communication between I and K is done through proactive way. ZRP consist of three parts IARP proactive part, IERP reactive part of it and BRP used with IERP to reduce the query traffic.

III. Misbehaving Nodes

Misbehaving nodes [7] are the nodes that pretend to be alright and cooperative but drops the data which is meant to pass on, also it gives an impression that it has performed the task appropriately and efficiently. Misbehaving nodes in a MANET affects the performing determining parameter of the routing protocols. These actions result in defragmented networks, isolated nodes, and drastically reduced network performance.

Results of Misbehaving Node leads to:-

Presence of misbehaving nodes in a network results in:

a) **Denial of service**: The DoS attack [9] results when the network bandwidth is hijacked by a malicious node. It has many forms: the classic way is to flood any centralized resource so that the network no longer operates correctly or crashes. For instance, a route request is generated whenever a node has to send data to a particular destination. A malicious node might generate frequent unnecessary route requests to make the network resources unavailable to other nodes.

b) **Black hole**: In this attack, a malicious node [7] uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. We provide a detailed description here in.

c) **Information disclosure [10]**: The malicious node may leak confidential information to unauthorized users in the network, such as routing or location information. In the end, the attacker knows which nodes are situated on the target route.

d) **Energy consummation [9]**: Energy is a critical parameter in the MANET. Battery-powered devices try to conserve energy by transmitting only when absolutely necessary. An attacker can attempt to consume batteries by requesting routes or forwarding unnecessary packets to a node.

e) **Impersonation [10]**: A malicious node may impersonate another node while sending the control packets to create an anomaly update in the routing table.

f) **Routing table overflow [9]**: The attacker attempts to create routes to nonexistent nodes. The goal is to have enough routes so that creation of new routes is prevented or the implementation of routing protocol is overwhelmed.

IV. Experiment Configuration

All the simulation work is performed in QualNet wireless network simulator version 4.5 [11]. Initially number of nodes are 50, simulation time was taken 180 seconds and seed as 1. Seed is a template in QualNet 4.5, in which nodes are placed in network. There are different templates are available in QualNet simulator with different seed number. All the scenarios have been designed with a terrain 1500m x 1500m. Mobility model used is Random Way Point [9] (RWP). In this model a mobile node is initially placed in a random location in the simulation area. For simulation, speed of node is varying from 10mps to 50mps. All the simulation works were carried out using three routing protocols (DSR, ZRP, and STAR) with varying speed of node. Network traffic load is provided by constant bit rate (CBR) application. A CBR traffic source provides a constant stream of packets throughout the whole simulation, thus further stressing the routing task.

There are four measurements in our experiments were defined as follows:

1) *Throughput (bits/s):*- Throughput [9] is the measure of the number of packets successfully transmitted to their final destination per unit time.

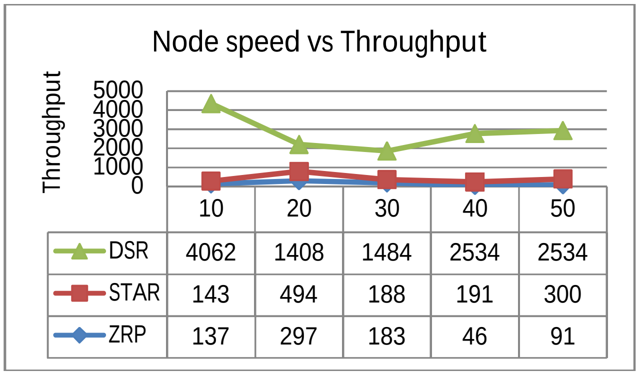
2) *Total Packets received:* - Packet delivery ratio **[6]** is calculated by dividing the number of packets received by the destination through the number of packets originated by the application layer of the source (i.e. CBR source).

3) End-to-end delay: Average End to End Delay **[6]** signifies the average time taken by packets to reach one end to another end (Source to Destination)**.**

*4) Average Jitter Effect***:** Signifies the Packets from the source will reach the destination with different delays [5]. A packet's delay varies with its position in the queues of the routers along the path between source and destination and this position can vary unpredictably.

V. Simulation Results & Analysis

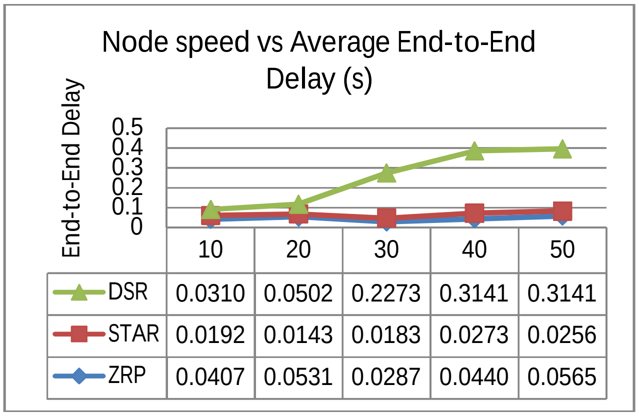
The simulation for these routing protocols is based on simulation time, number of node, area of network, speed of node, routing protocols, and pause time. In experimental methodologies performance of routing protocols will be measured with variation in speed of node in network while rest of all other parameters like simulation time, area of network, and speed of node is kept constant. Effects of different parameter on performance of on-demand protocols are exposed below.



	10	20	30	40	50
DSR	4062	1408	1484	2534	2534
STAR	143	494	188	191	300
ZRP	137	297	183	46	91

Figure 4: Node Speed vs Throughput

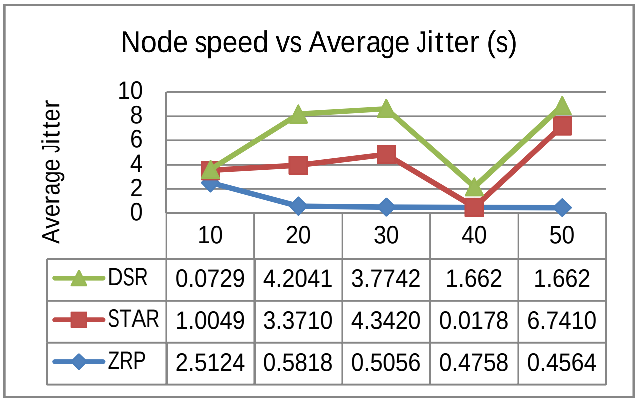
In above graph it can be observed that throughput of DSR is better than STAR and ZRP. Due to enhance mechanism of route table and better signal strength DSR perform well in above scenario.



	10	20	30	40	50
DSR	0.0310	0.0502	0.2273	0.3141	0.3141
STAR	0.0192	0.0143	0.0183	0.0273	0.0256
ZRP	0.0407	0.0531	0.0287	0.0440	0.0565

Figure 5:-Node speed vs Average End-to-End Delay

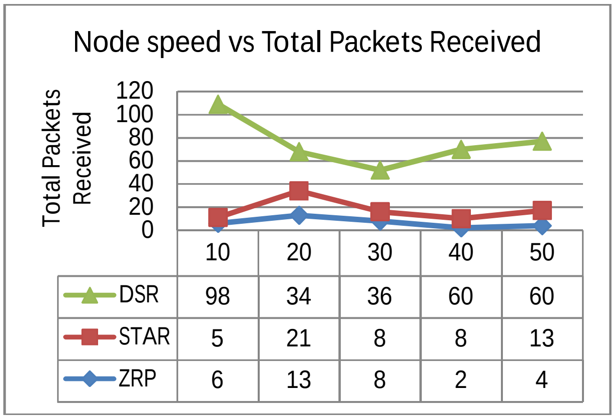
In above graph it can be observed that calculation of End-to-End delay for DSR is well than STAR and ZRP.



	10	20	30	40	50
DSR	0.0729	4.2041	3.7742	1.662	1.662
STAR	1.0049	3.3710	4.3420	0.0178	6.7410
ZRP	2.5124	0.5818	0.5056	0.4758	0.4564

Figure 6:-Node Speed vs Average Jitter

Due to better route cache, average jitter of DSR is better than STAR and ZRP as shown in figure 6.



	10	20	30	40	50
DSR	98	34	36	60	60
STAR	5	21	8	8	13
ZRP	6	13	8	2	4

Figure 7:- Node speed vs Total Packet Received

From the above graphs it is observed that performance of DSR is superior to ZRP and STAR. So, DSR is used when some misbehaving node is present in network.

DSR can perform well when nodes in network are moving with speed of 10 mps to 50 mps. The coverage and signal strength is affected due to speed of nodes. But from figure 7, it can observe that server can receive most packets when DSR is used.

VI. Conclusion

This paper is focus on the performance of three routing protocols DSR, ZRP and STAR in presence of some misbehaving node in the network. After various analysing results with variation in the speed of node in network it's observed that DSR is more suitable for routing in the presence of misbehaving nodes in the network as compared to the other routing protocols selected of different genre. So DSR is used when some misbehaving node is present and nodes in network moving with speed of 10 mps to 50 mps.

References

[1] Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu .Mobile ad hoc networking: imperatives and challenges, School of Engineering, University of Texas at Dallas, Dallas, TX, USA ,b Istituto IIT, Consiglio Nazionale delle Ricerche, Pisa, Italy ,c Department of Computer Science, University of Texas at Dallas, Dallas, TX, USA. Ad Hoc Networks 1 (2003).

[2] Charles E. Perkins, "Mobile Ad-Hoc Networks,"Addison-Wesley, 2000.

[3] Elizabeth M. Royer, University of California, Santa Barbara Chai-Keong Toh, Georgia Institute of Technology, A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks.

[4] Zygmunt J. Haas, Cornell University Marc R. Pearlman, Cornell University the Zone Routing Protocol (ZRP) for Ad Hoc etworks draft-ietf-manet-zone-zrp-02.txt> 2001.

[5] D. Johnson, Y. Hu, and D. Maltz. The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4. RFC 4728 (Experimental), Feb. 2007.

[6] Layuan, Li Chunlin, Yaun Peiyan "Performance evaluation and simulation of routing protocols in ad hoc networks", February 2007, Computer Communication.

[7] Abdelaziz Babakhouya, Yacine Challal, Abdelmadjid Bouabdallah, A Simulation Analysis of Routing Misbehaviour in Mobile Ad hoc Networks. 2008 IEEE, DOI 10.1109/NGMAST.2008.56.

[8] Y. Hu, A. Perrig, and D. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. WirelessNetworks, 11(1):21–38, 2005.

[9] D. Djenouri, A. Derhab, and N. Badache. Ad hoc networks routing protocols and mobility. Int. Arab J. Inf. Technol.3 (2):126–133, 2006.

[10] P. Michiardi and R. Molva. Simulation-based analysis of security exposures in mobile ad hoc networks. *European Wireless Conference*, 2002.

[11] Scalable Network Technology, "QualNet4.0 simulator" tutorial and QualNet Forum, http://www.scalable-networks.com/forums/.....