International Journal of Advanced Technology in Engineering and Science
Vol. No.9, Issue No. 05, May 2021
www.ijates.com
ijates
ISSN 2348 - 7550

Routing Misbehavior and Performance Analysis in Mobile Ad hoc Network

[1]Rakesh Gupta, [2]Prashant Singh , [3]Amit Kumar Pandey,[4]Dhyanender Jain

[1,2,3,4] Department of Information Technology

[1,2,3,4] Dr. Akhilesh Das Gupta Institute of Technology & Management, New Delhi, India.

guptarakesh013@gmail.com[1],prashant.ert@gmail.com[2],amitpandey33@gmail.com[3], dhyanendra.jain@gmail.com[4]

Abstract

MANET is a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure. In general, routing protocols for MANETs are designed based on the assumption that all participating nodes are fully cooperative. However, due to the lack of infrastructure and scarcely available battery-based energy, node misbehaviors may exist in the network. In this paper, we have discuss the impact of routing misbehavior over end-to-end delay, throughput and delivery ratio through simulation.

1. Introduction

Mobile Adhoc Network is a collection of co-operative mobile nodes communicating with each other through wireless links, without support of any existing infrastructure [1, 2, 3].As for the mode of operation, adhoc networks are basically peer-to-peer multi- hop mobile wireless networks where information packets are transmitted in a store and forward manner from a source to an arbitrary destination, via intermediate nodes. As the node move, the resulting change in network topology must be made known to the other nodes so that outdated topology information can be updated or removed .In MANET nodes are free to move arbitrarily with different speeds thus, the network topology may change randomly and at unpredictable times. All the nodes in MANET behave as routers that take part in route discovery and maintenance of paths to other nodes in the network. The conventional routing protocols for ad hoc protocols treat each mobile host as a router. Because there is no administrative node in wireless adhoc networks, most network algorithms are based on the collaboration between nodes to co-operate with each other, trust between nodes is essential, but it is hard to achieve in practice. so the wireless ad hoc network is inherently vulnerable. On the other hand, ad hoc network in the presence of nodes that agree to forward packets but fail to do so. For example node can become selfish and refuse to forward data packets to other nodes, or the node fails to forward data packets to the destination node. Finally, a node could enter an inactive state,

(i) because of a limited power supply. Misbehaving nodes cause problems.
(ii) overhead—lacks CPU cycles, buffer space, or network bandwidth to forward packets.
(iii) selfish--unwilling to spend battery life, CPU cycles, or network bandwidth.
(iv) malicious-drops packets for denial of service attack (v) broken-Software fault keeps from forwarding packets.

There are many routing algorithm exists for ad hoc network. We selected DSR routing algorithm for performance analysis with routing misbehavior. Dynamic Source Routing (DSR) algorithm is an innovative approach to routing in a MANET in which nodes communicate along path stored in source routes carried by the data packets. We studied DSR. Dynamic Source Routing Protocol (DSR) provides simple and efficient routing for multihop ad hoc network of mobile nodes. It uses Source routing instead of relying on the routing table at each intermediate device. This protocol is truly based on source routing whereby all the routing information is maintained (continually updated) at mobile nodes. It has only two major phases, which are Route Discovery and Route Maintenance. Route Reply would only be generated if the message has reached the intended destination node (route record which is initially contained in Route Request would be inserted into the Route Reply).To return the Route Reply, the destination node must have a route to the source node. If the route is in the Destination Node's route cache, the route would be used. Otherwise, the node will reverse the route based on the route record in the Route Request message header (this requires that all links are symmetric). In the event of fatal transmission, the Route Maintenance Phase is initiated whereby the Route Error packets are generated at a node. The erroneous hop will be removed from the nodes route cache;all routes containing the hop are truncated at that point.Again the route Discovery phase is initiated to determine the most viable phase.

2. Related work

A Mobile Ad-hoc network consists of nodes that move arbitrarily and form dynamic topologies. The nature of open structure and scarcely available battery based energy, node Misbehavior may exist in MANETs due to the presence of selfish nodes.Most common types of denial-of service attacks are categorized by the researchers [4][5][6][7] discussed here in brief.

Rushing Attack—In an on demand routing protocols, whenever source nodes flood the network with the Route Request packets in order to discover the new routes to the destination, each intermediate forwarding node processes the first Route Request packet from a particular node to suppress the duplicate forwarding. It discards the duplicate packets that arrive later. A rushing attacker by skipping some of the routing or MAC layer process can quickly forward these packets. As a result it gains the access of valid routes further data transmission .All most the on-demand routing protocols are prone to the rushing attacks[4]

Black hole Attack—In black hole attack[6],an attacker first introduce itself in the forwarding group and then instead of forwarding the data packet to the destination, it drops all the packets it receive resulting a poor packet delivery ratio.

Wormhole Attack—in this type of attack [5], after gaining access to the forwarding groups, an attacker simply forwards the control packets received to a particular node.

Jellyfish Attack—after gaining the access of the forwarding group, the attacker in this case, delayed the packet forwarding process for a certain period of time, resulting in a high end-to-end delay [5].

3. Simulation & Result Analysis:

DSR utilizes a specially designed framework which builds on the Global Mobile Information System Simulator (GloMoSim).Global Mobile Information System Simulator (GloMoSim) is a scalable simulation environment for large wireless and wireline communication networks [8].GloMoSim simulates networks with up to thousand nodes linked by a heterogeneous communications capability that includes multicast communications using direct satellite broadcasts, multi-hop. GloMoSim also is a scalable simulation library for wireless network systems built using the PARSEC simulation. PARSEC (for Parallel Simulation Environment for Complex systems) is a C-based simulation language developed by the Parallel Computing Laboratory at UCLA, for sequential and parallel execution of discrete-event simulation models[9]. PARSEC runs on several platforms, including most recent UNIX variants as well as Windows. PARSEC is designed to cleanly separate the description of a simulation model from the underlying simulation protocol, sequential or parallel, used to execute it.

The following parameters are used in the simulation-

Parameters	**Values**
Number of nodes	50
Simulation time	500 Seconds
area	500*500m^2
Number of connections	8
Transmission power	15dBm
Number of malicious node	Variable(110)
velocity	20s

By using the parameters given in the above table, we can evaluate the performance of DSR Through these performance matrices: (i) Throughput: Number of packets that are reached to destination per second. (ii) Packet Delivery Ratio (PDR) is the ratio between the number of packets transmitted by source and the number of packets received by destination. It measures the loss rate. A high packet delivery ratio is desired in any network. (iii) End-to-End delay: This is the time from the generation of the packet in the sender up to its reception at the destination.

Simulation carried out varying the network size from nodes 20, 40, 60, 80, 100 and the velocity of the nodes have range between 0 to 20m/s. with these metric we have calculated the throughput, delivery ratio and end-to-end delay.

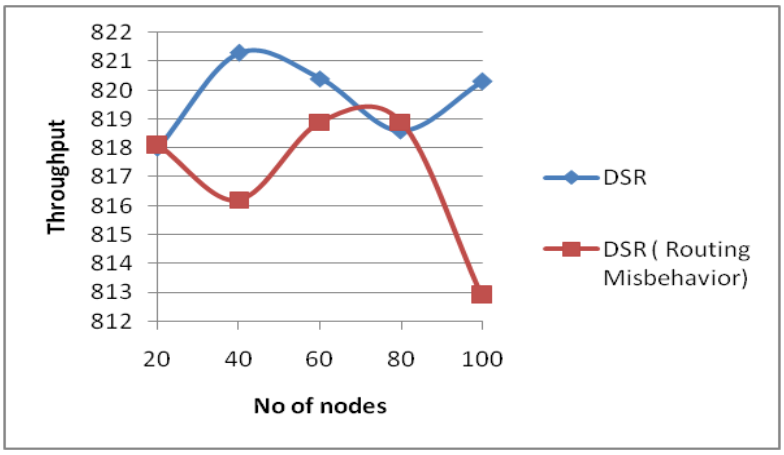

Fig 1 Throughput vs. Nodes

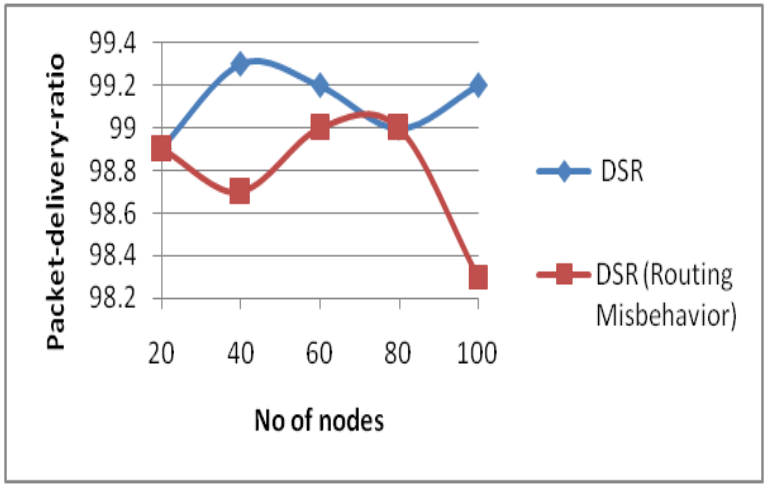

Fig.2 Delivery-ratio vs. Nodes

The above figure 1 shows the throughput vs. no of nodes. As we compare both the throughput. Throughput with DS Protocol and throughput with DSR protocol (Routing Misbehavior), throughput DSR increase as the no of nodes increase in Ad hoc network. The above figure 2 shows the Packet-delivery-ratio vs no of nodes .As we compare packet delivery ratio with DSR Protocol, and Packet delivery Ratio DSR(Routing Misbehavior) , Packet-delivery-Ratio with DSR (Routing Misbehavior),

Decrease when no of nodes in increase in mobile ad-hoc network.

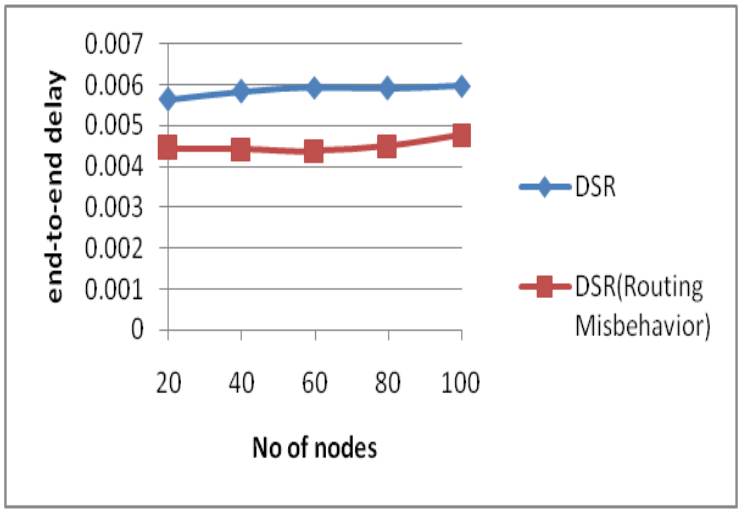

Fig.3 End-to-End Delays vs Nodes

The above figure 3 shows the end –to-end delay vs. No of nodes. As we compare the end-to-end delay with DSR Protocol and end-to-end delay with DSR (Routing Misbehavior), end-to-end delay increase in case of DSR (Routing Misbehavior).

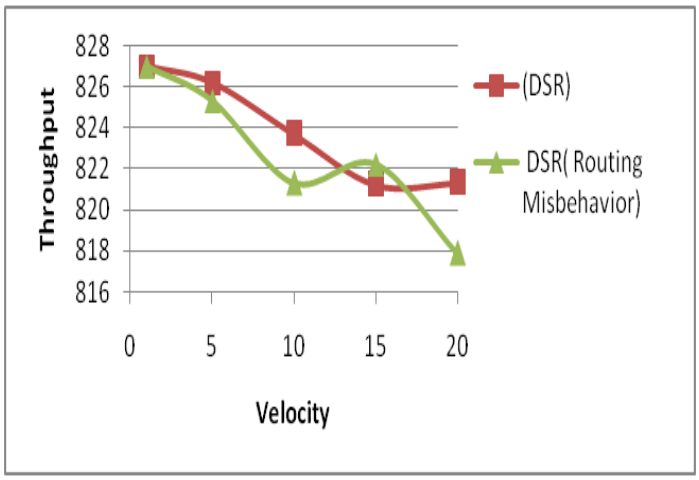

Fig 4.Throughput vs. Velocity

fig.4 shows the throughput vs. velocity. As we compare the throughput with DSR protocol and throughput with DSR (Routing Misbehavior). Throughput with DSR protocol increase as the velocity increase.

fig.5 shows the packet-delivery-ratio vs. velocity .As we compare the packet-delivery-ratio with DSR and packet-delivery-ratio with

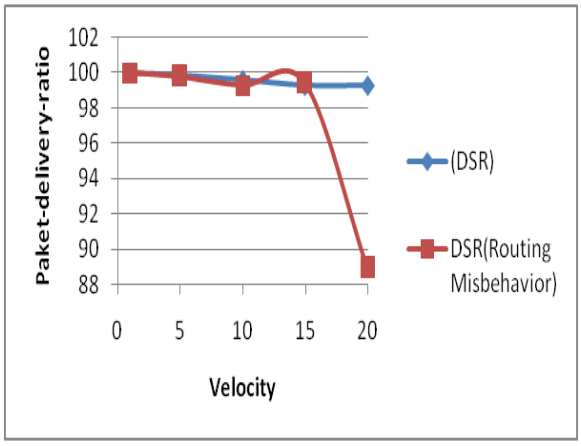

Fig 5 Delivery ratio vs. Velocity

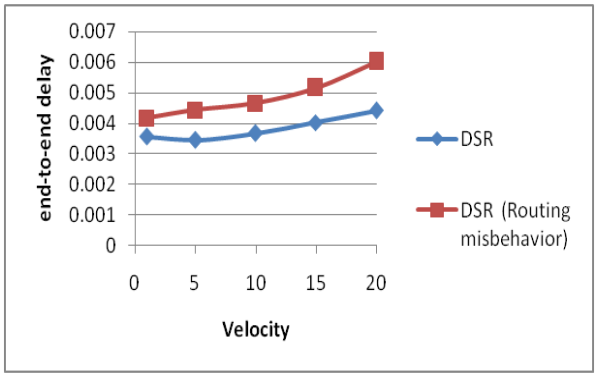

Fig.6 End-to-End delay vs. Velocity

The Above fig.4 shows the throughput vs.velocity.As we compare the throughput with DSR protocol and throughput with DSR (Routing Misbehavior). Throughput with DSR protocol increase as the velocity increase.

The Above fig.5 shows the packet-delivery-ratio vs.velocity. As we compare the packet-delivery-ratio with DSR and packet-delivery-ratio with DSR (Routing Misbehavior).packet delivery ratio with DSR increase when velocity increase.

Fig.6 shows the end-to-end delay vs. velocity. As we compare the end-to-end delay with DSR and end-to-end with DSR (Routing Misbehavior).end-to-end delay with DSR(Routing Misbehavior) increase as the velocity increase in Mobile Ad hoc network.

4. Conclusion and Future Work

This paper describes how the routing misbehavior affects the network performance. We have analysis the misbehavior, varying network size and velocity of nodes. Routing misbehavior

adversely affect the throughput, delivery ratio and end-to-end delay. Future work is required to develop a model to find a routing misbehaving nodes and remove these nodes from the network. So that efficiency of routing algorithm will increase.

References:

1) HadiSargolZaey, AyyoubAkbariMoghanjoughi and SabiraKhatun,--AReview and Comparison of Reliable Unicast Routing Protocols For Mobile Ad Hoc Networks,IJCSNS International Journal of Computer Science and Network Security,VOL.9 No.1,pp.186-196, January 2009.
2) MobileAdhocNetworks(MANET),http://www.ietf.org/html.charters/manetcharater.html.(1998-11-29)
3) J.P. Mackerand M.S.Corson,''Mobile Ad Hoc Networking and the IETF".ACM SIGMOBILE Mobile Computing and Communications Reviews,Vol.2,No.2, pp. 9-14, January 1998.
4) Y.C Hu,APerrig and D.B.Johnson "Rushing Attacks and Defense in Wireless Ad Hoc Networks Routing Protocol";Proceeding of ACM Wise2003,sep,2003
5) Hoang Lan Nguyen and Uyen Nguyen" Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks". Proceedings of the International Conference of Networking, International Conference of Mobile Communication and Learning Technologies.
6) Tamilselvan, L. Sankaranarayanan, V. "Prevention ofBlackhole Attack in MANET ".Proceedings of the 2nd International Conference on wireless Broadband andUltraWidebandCommunications,2007.(AusWireless2007).
7) Yih-Chun Hu Adrian Perrig and David B.Johnson ,"Packet Lashes: A Defence against Wormhole Attacks in Wireless Ad Hoc Networks"Proc.of the 22nd Conf .of the IEEE Computer and CommuniationSocities (INFOCOM).2003.
8) GloMoSim: Global Mobile Information Systems SimulationLibrary.http://pcl.cs.ucla.edu/projects/glomosim/.
9) R. Bagrodia, R. Meyer et al., "PARSEC: A Parallel Simulation Environment for Complex Systems," IEEE Computer, October 98.