Analyzing the Effect of Constant and Lognormal Shadowing Model on Ad-hoc Routing Protocols

Gaurav Sharma
M.Tech Student,
SHIATS, Allahabad

Vaishali Sahu
M.Tech Student,
MNNIT, Allahabad

Prashant Kumar Maurya
M.Tech Student
SHIATS, Allahabad

Rajeev Paulus
Assistant Prof.
ECED, SSET, SHIATS

ABSTRACT
Over recent years, with the increasing use of laptops, iPods', PDA, etc. the demand for ad-hoc networks has been increased. Mobile ad-hoc network (MANET) is a network used to provide communication among various devices without any need for pre-existing infrastructure. MANET is formed by mobile nodes connected by wireless links without access points and backbone networks. It can be used for various applications as disaster management, conferences, military operations, rescue operations, and many more. Routing Protocols, other than conventional protocols are required for routing purposes in MANET. In this paper, performance of ad-hoc routing protocols as AODV, DSR and DYMO are analyzed under the effect of two shadowing model, as Constant and Lognormal.

Keywords
Mobile Ad-hoc networks, AODV, Constant Shadowing model, Lognormal Shadowing model, DSR, DYMO.

1. INTRODUCTION
Over recent years, with the upcoming of mobile Laptops, tablets, and mobile phones, there is often a requirement to set up a network to enable communication among some of these devices. For movable devices, a wireless network is required. Wireless networks can be of two types one with infrastructure or other is without pre-specified infrastructure. MANET is a temporary network that is designed for data communication among various mobile nodes, without any requirement of fixed or pre-specified infrastructure. Each node is itself a router in this type of network. Field of application for MANET is the area, where a temporary communication among some nodes is required. In a MANET, the concern nodes are not familiar with the topology of the network, since the nodes are mobile, due the fact, the topology of the network changes continuously. Nodes can move with random velocity and in random direction too, or for some nodes movement can be uniform. In fact, all of the changes are not predictable in a MANET. All the nodes have to identify the topology of the network. A new node can introduce itself into a network by using the process of broadcast. A MANET can be used for both unicast and multicast type of communication. Conventional protocols used for fixed infrastructure networks cannot be efficiently used for mobile ad-hoc networks, so that MANET requires routing protocol other than conventional ones. The available protocols for MANET are, as, DSR [4], AODV [1, 2, 3], OLSR [7], FSR [8], TORA [6], ZRP [9], etc., The protocols which are taken for analysis in this paper are discussed in section II. The overview of the paper is as: the introduction is given in Section I; Overview of Protocols is given in Section II; Simulation setup is included in Section III. Results and discussion is specified in Section IV, section V is all about conclusion.

2. OVERVIEW OF PROTOCOLS
2.1 Ad-hoc On Demand distance Vector routing protocol (AODV) comes in the category of Reactive routing protocols. In reactive protocols routes are discovered and created on demand. The other category is proactive, in which each node has to maintain tables containing information about all the nodes in the network. In this category, periodical updates are necessary along with the updates whenever there is a change in the topology of the network. Periodic global broadcasting increases the control message and bandwidth requirements [1].

Since AODV is reactive routing protocol, then for this protocol nodes never participate in periodic global routing-table exchange [2]. When a node wants to communicate to another node, then only it finds a route to that node. Nodes discover other nodes in its neighborhood by locally broadcasting a packet called Hello message [1] with Time-to-live value of 1. To initiate the route discovery, the source node broadcast a route request (RREQ) [1, 5] packet to its neighbors. The Route Request packet contains the following parameters as: address of the source, request identity, address of the destination, and sequence number of the source. Beside these parameters sequence number of the destination and hop-count are also there. The addresses of the destination and source are the IP addresses for destination and source nodes respectively. When a source node generates a fresh Route Request a counter is incremented which is called Request Identity. Hop count is counter initially set to zero and incremented after each hop. Whenever an intermediate node gets a RREQ, it checks the source address and request id to detect whether it is a new request or a duplicate [5]. If duplicate, it is discarded; if fresh, table update is done. The intermediate node compares the destination sequence numbers in the received RREQ packet with the stored one in its route-entry. If the sequence number in the RREQ packet is greater than or equal to the stored one, then RREQ is rebroadcasted, also the greater sequence number is updated in the route entry; otherwise it unicasts RREP (Request Reply) packet [1] back to the source via the node from which it received RREQ to declare that it has a valid route to the destination. With the traverse of RREQ, reverse pointers [1] were set up from all intermediate nodes towards the source node. As RREP travels towards the source, each node in the path sets up a forward pointer [1], and also updates its table.

As the RREPs are propagated back for a particular source node towards that source node; other replies are also propagated for the same source, if in the case these RREPs have the sequence number of the destination, greater than or equal to the previous one, with a smaller hop count; otherwise these are discarded [1]. Thus resulting in the decrease of redundant replies and confirming the latest routing information. When the first RREP is received by the source node, data transmission is initiated; but in future if a fairer option is available for the route, then this option is chosen immediately and routing table can be updated quickly [5].

Link breakage is obvious in mobile networks, which invokes the need of path maintenance [3]. In the case of link failure during an active session, the node upstream [3] of the breakpoint, broadcasts the RERR (Route Error) [3] message. In this way RERR propagates back to the source node, which in turn re-initiates path discovery process if it still requires.

2.2 Dynamic Source Routing (DSR)

Dynamic Source Routing (DSR)[4] is also reactive routing protocol, but the concept used is explicit source routing. In this routing protocol data packet which are sent contains the complete, sequenced array of all the nodes via which each data packet has to go through to reach to the destination. The benefit of including the source route within the header of packets of data is that, other nodes which want to send these packets in future can store and use this routing information. Normally, the sender will obtain a suitable source route by searching its Route Cache of routes previously learned; if no route is found in its memory, a protocol termed as route discovery is started to dynamically find a new route to this destination node. To initiate the Route Discovery, source node sends a route request message, to the nodes which are lying in current transmission range of the source node [4]. Each Route Request message identifies the initiator and destination of the process. This locally broadcast message contains a request identification number which is unique in itself, and that identification number is given by the initiator. It also possess a recorded list of all the address for each intermediate node through which this particular copy of the Route Request message has been forwarded [4]. If a request arrives at a node and the concern node is the target of the discovery process, then the node immediately returns a reply to the node which is the initiator of the process. In this way the concern node provides a recorded route copy from the request of the route; when the source node receives reply from the target node, it saves the provided path in its memory (Route Cache) for use in sending subsequent packets to the target. If the node receives the request which has the same request identification number as of previous ones, then it will discard the current request [4]. The request is also discarded if the address of the node at which request is arrived, is found in it, otherwise the node appends its own address to the route record in the request message and propagates it by transmitting it as a local broadcast packet with the similar request identification number. While propagating the reply back to the source node of the Route Discovery process, destination replying back to source, will typically examine its own Route Cache for a route back to source, and if found, will use it for the source route for delivery of the packet containing the reply message, if the condition does not satisfy, the destination can initiate the process of discovery for source node but to avoid count to infinity problem, it must the concept of piggybacking. In the process reply message is piggybacked onto the request message initiated by it for the concern source [4].

2.3 DYMO

The Dynamic MANET On-demand routing protocol (DYMO) [16] enables on-demand, multi-hop unicast routing among routers in mobile ad-hoc networks. The basic operations of the protocol are route discovery and route maintenance. Route discovery is initiated when a node or router has to transmit a packet towards a target or destination node and it is not aware of the path to the target. Route maintenance is a process that is used to maintain the link between the source and destination nodes and eventually to avoid the loss of data packets. During route discovery, a router initiates flooding of a Route Request message (RREQ) throughout the network to find a route to a particular destination, via the router responsible for this destination [16]. During this hop-by-hop flooding process, each intermediate router receiving the RREQ message records a route to the originator. When the router of the destination node receives a request message for the route, it copies the path to the initiator and immediately answers with a reply message (RREP) towards the initiating source router [16]. When the source router gets the reply message, then route is established between the routers of source and destination bi-directionally. Route maintenance [16] takes place when a node receives a packet to forward it to the destination and a route for the destination is not known or the route is broken, then the router of the source of the packet is notified. A Route Error (RERR) [16] is transmitted to indicate the route to one or more affected destination addresses is Broken or missing. When the source's router receives the RERR, it marks the route as broken. Before a router can forward a packet to the same target, it must follow the process of discovery for a route to the concern destination one more time.

3. SIMULATION SETUP

Many researchers [12, 13, 14, 15, 17] have worked on routing protocols for MANET, and analyzed these protocols extensively, however, in this paper we have studied the performance variation of AODV, DSR and DYMO by changing the maximum speed of nodes with which it can move in the network, over an area of 700×700 m^2. Beside this change shadowing model has been changed with variation in maximum speed of nodes. Among various nodes application of Constant Bit Rate is applied. All the nodes in the depicted scenario are given a mobility using the protocol of RWP mobility model. Two Shadowing models used here are Constant (CSM) and Log-normal (LNSM) shadowing model. A signal is attenuated while propagating due to the obstruction in the path. The shadowing model is a process to measure the degree of attenuation. The CSM is suited for the scenarios when mobility is not applicable for the nodes (users) or where the obstructions through the propagation paths remain constant. While, LNSM is suited for the condition in which mobility is applicable for the nodes or users and obstructions are there while traversing. In LNSM, a log-normal distribution is used for the value of shadowing with a standard deviation specified by the user. In general, for LNSM the concern value ranges between 4 and 12 dB depending upon the density of obstructions within the traversing environment. The scenario parameters are briefly depicted in Table 1. The simulations are done with the help of a network simulator, called Qualnet 5.2 [11]. It is a simulator used to analyze the performance of wired, wireless, and heterogeneous networks. It allows designing network models easily, efficiently coding protocols, and run models that present real-time statistics.

After obtaining the simulation results parameters as PDR, Average end-to-end delay, throughput, and average jitter are analyzed.

3.1 Packet delivery ratio

It is the fraction of number of packets received by the target node to the number of packets sent by the source node. It is the measure of reliability for a particular protocol and network used.

3.2 Throughput
It is defined as the information in bits which is received successfully by the destination in an average time. Its unit is bps.

3.3 Jitter
It is defined as the change in the time of the arrival for the packets at the receiver end.

3.4 End-to-End delay
It is the time elapsed when a packet is sent from the source node and is successfully received by the destination node. It includes delays as delay for route discovery, propagation time, data transfer time, and intermediate queuing delays.

TABLE 1

Parameter	Value
Simulation time	101 seconds
Number of Channel	1
Channel frequency	2.4 GHz
Path loss model	Two-Ray
Mobility model	Random-waypoint
MAC protocol	IEEE 802.11
Physical layer Radio-type	IEEE 802.11b
Packet size	512 bytes
Pause Time	25 seconds
Number of nodes	75
Rate of transmission of packets	5 packet per second
Transport layer protocol	UDP
Maximum Speed	2, 5, 10, 15, 20 mps
Minimum Speed	0 mps

4. RESULTS AND DISCUSSION
In fig. 1, throughput is shown against maximum speed of nodes for all the concern cases. AODV performs better in all the cases, compared to other protocols in constant shadowing model. As speed is increased, the throughput is increasing for AODV-Constant. Performance of DSR is worst for constant shadowing model. DYMO performs in between the two protocols. For log-normal shadowing model, findings are crucial, since, DSR performs better than the two protocols. In this case AODV is performing badly than two protocols. Overall, taking all the cases AODV has higher throughput in constant shadowing model case.

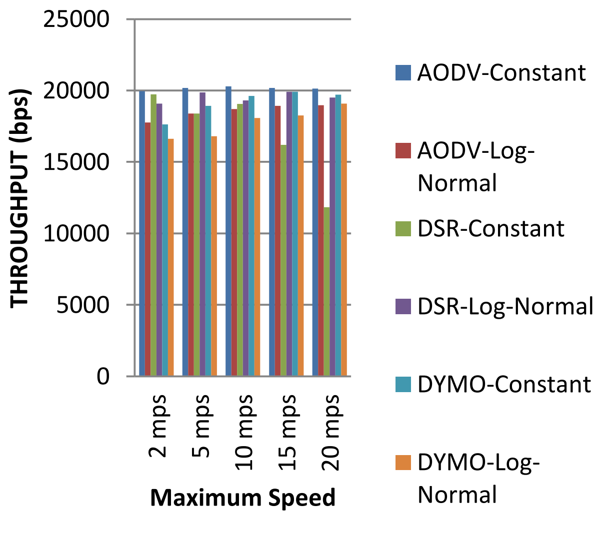

Fig. 1 Throughput vs Maximum Speed

In fig. 2, Average Jitter is plotted against maximum speed of nodes for all three protocols and two shadowing models. For constant model, AODV has lowest jitter and DSR has worst performance. For 20 mps, average jitter increases to a large value. Again DYMO performs better than DSR but not good as AODV and the same pattern is observed with log-normal shadowing model but DSR does not perform so badly as in constant model. As speed of nodes is increasing the jitter is observed to increase for all the simulated cases.

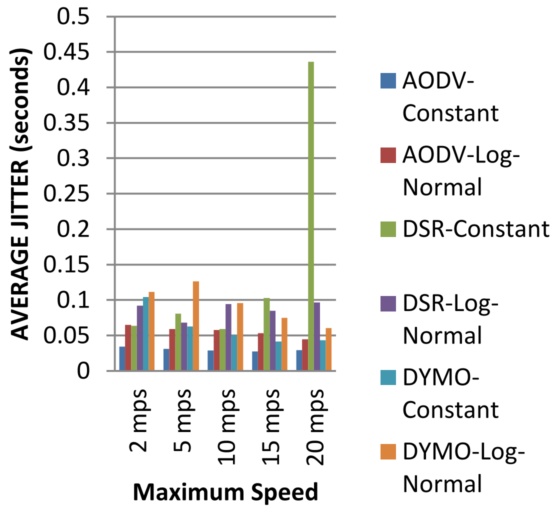

Fig. 2 Average Jitter vs Maximum Speed

In fig. 3, Average end-to-end delay is shown against maximum speed of nodes for both the shadowing models, the average delay is too small for AODV and DYMO, and it is decreasing with increase in speed, but for DSR especially in constant shadowing model, performance of DSR is unacceptable.

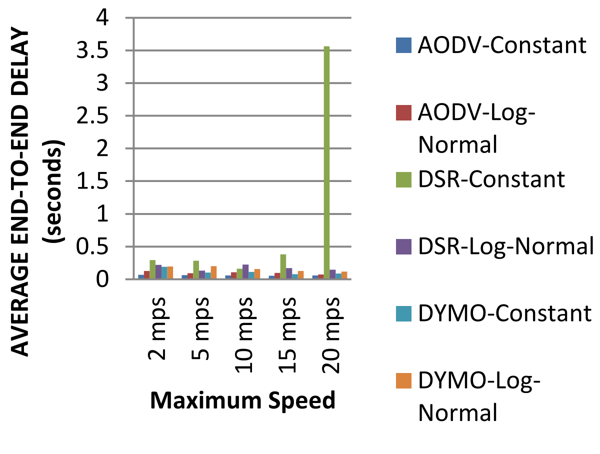

Fig. 3 Avg. End-to-end delay vs Maximum Speed

In fig. 4, packet delivery ratio is shown against maximum speed of nodes for all the concern cases. AODV performs better in all the cases, compared to other protocols in constant shadowing model. The PDR is not much affected for AODV-Constant. Performance of DSR is worst for constant shadowing model; and, it is getting worse with increase in speed. DYMO performs in between the two protocols and its performance increases with increase in speed. For log-normal shadowing model, DSR performs better than the two protocols. In this case AODV is performing badly than two protocols. However, performance is increasing with speed for log-normal model. Overall, taking all the cases AODV has higher PDR in constant shadowing model case.

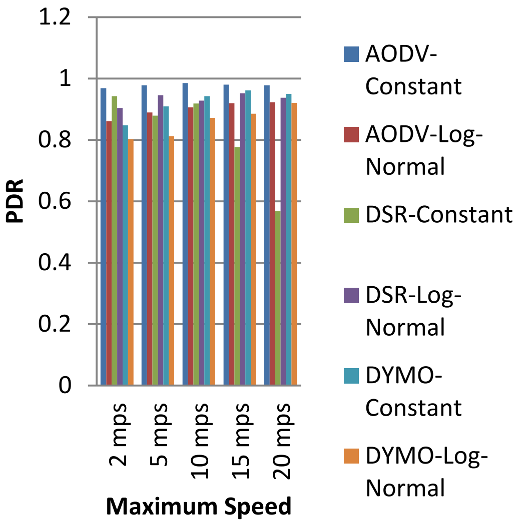

Fig. 4 PDR vs Maximum Speed

5. CONCLUSION

In this paper, the performance of various routing protocol, as AODV, DYMO and DSR are evaluated on the basis of changing speed for mobile nodes. The maximum speed of nodes is changed from 0 mps to 20 mps and parameters such as Throughput, PDR, Average Jitter, and Average Delay are analyzed. The trio of routing protocols is simulated for two of the shadowing model, Constant, and Log-normal model.

It is observed that for constant model AODV outperforms the other the two protocols. DSR shows the worst performance. But for the log-normal, DSR shows better performance than AODV and DYMO.

6. REFERENCES

[1] C.E. Perkins and E.M. Royer, "Ad-hoc On-Demand Distance Vector Routing", Proceeding of 2nd IEEE Workshop, Mobile Computing System Applications, pp:90-100, 1999.

[2] C.E. Perkins, E.M. Royer, and S Das, "Ad-hoc On-Demand Distance Vector (AODV) routing", IETF MANET Working Group, 2000.

[3] E.M. Royer and C.E. Perkins, "An Implementation Study of the AODV Routing Protocol", 2000.

[4] Josh Broch, David Jhonson, and David Maltz, "The dynamic source routing protocol for mobile adhoc networks for IPv4" IETF RFC 4728, Feb 2007.

[5] A.S. Tanenbaum, "Computer Networks" 4th edition, Pearson

[6] V. Park and S. Corson, "Temporally-Ordered Routing Algorithm (TORA) version 1 Functional Specification", draft-ietf-manet-tora-spec-04.txt.July 2001.

[7] Philippe Jaquet, Paul Muhlethaler and Amir Qayyum, 2001. "Optimized Link State Routing Protocol", IETF Draft, draft-ietf-manet-olsr-06.txt.

[8] G. Pei, M. Gerla and T.W. Chen, "Fisheye State Routing in Mobile Ad-hoc Networks", in proceedings of the 2000 ICDCS workshops, Taipei, Taiwan, April 2000.

[9] Zygmunt J. Haas, Mark R. Pearlman, and Prince Samar, "The Zone Routing Protocol (ZRP) for Adhoc Networks", draft-ietf-manet-zone-zrp-04.txt.July 2002.

[10] Perkin C, Bhagwat P, "Highly Dynamic Destination Sequenced Distance-Vector Routing", SIGCOMM 94, Computer Communication Review, vol. 24, no. 4, pp: 234-244, October 1994.

[11] Qualnet Network Simulator; http://www.scalacble-networks.com

[12] Md. Arafatur Rahman, Farhat Anwar, Jannatul Naeem, and Md. Sharif Minhazul Abedin, "A Simulation based Performance Comparison of Routing Protocol on Mobile Ad-hoc Network (Proactive, Reactive, and Hybrid)", ICCCE, IEEE, 2010.

[13] M. Bhourma, H. Bentaouit, and A. Boudhir "Performance Comparison of Ad-hoc Routing Protocols AODV and DSR", IEEE, 2009.

[14] K. Amzad and A. J. Stocker, "Impact of Node Density and mobility on the performance of AODV and DSR in MANETs", CSNDSP, IEEE 2010.

[15] V. Kumar, S. Jain, and S. Tiwari, "Impact of Node Density and Mobility on Scalable Routing Protocols in Mobile Ad-hoc networks", Special Issue of IJCA, 2012

[16] C. Perkins and I. Chakerers, "Dynamic MANET On-demand routing protocol (DYMO) for mobile adhoc networks" IETF Draft, Oct 2012.

[17] V. Sahu, G. Sharma, and R. Paulus, "Study of Performance Variation of AODV Routing Protocol for Various Parameter Patterns using Qualnet Simulator", volume-54, no. 6, pp. 7-11, September, 2012, IJCA (0975-8887).