A Comparative Analysis on DSR and DSDV

Charmil N Bharti[1] Prof. Mihir Patel[2]
[1]P.G. Student [2]Assistant Professor
[1,2]Department of Computer Engineering
[1,2]Chhotubhai Gopalbhai Patel Institute of Technology, India

Abstract— In MANET the routing protocols are of three types reactive, proactive and hybrid. The reactive protocols establishes route from source to destination when required and in proactive routing protocols routes store routing tables and on that basis route between source and destination is established. DSR is one of the reactive type of routing protocol. On the basis of hop counts and sequence number the route is established between source to destination. Congestion may occur between source and destination. The purpose of this study is to learn DSR and DSDV protocol, congestion in DSR protocol and different method for congestion control. The simulation of DSR and DSDV protocols are performed in NS2. The average throughput of DSR and DSDV and comparison of DSR and DSDV protocol on the basis of throughput is shown.

Key words: DSR, DSDV, Congestion, Throughput

I. INTRODUCTION

MANETs is an IEEE 802.11 framework. It is an interconnected collection of wireless nodes where there is no networking infrastructure in the form of base stations, devices do not need to be within each other's communication range to communicate, the end-users devices also act as routers, nodes can enter and leave over time, data packets are forwarded by intermediate nodes to their final destination. Figure 1.1 shows the typical architecture of MANET.

Fig. 1: Mobile Ad-hoc Networks (MANETs)

Unlike a wired network, in these type of networks all the nodes are mobile or free to move independently to communicate with other nodes present in the network, so the topology changes very frequently. All the nodes here act like a router to provide multi hop routing which help nodes in communicating with each other [1]. Due to the lesser range of transmission of a node the communication between two nodes get information for routing through the several intermediate nodes to route a packet. Each node here can communicate directly to the node present in its transmission range via radio wave. Each node in MANETs takes routing decision independently without depending upon any central authority like for route selection, route request, route update and for creating a new communication link with their neighbours. Generally, on all nodes combined effort whole networks functionality is dependent.

II. CLASSIFICATION OF ROUTING PROTOCOLS OF MANETS

There are many ways to classify the MANET routing protocols, depending on how the protocols handle the packet to deliver from source to destination. But routing protocols are broadly classified into three types such as proactive, reactive and hybrid protocols.

A. Proactive Protocols:

These types of protocols are called table driven protocols in which, the route to all the nodes is maintained in routing table. Packets are transferred over the predefined route specified in the routing table. In this scheme, the packet forwarding is done faster but the routing overhead is greater because all the routes have to be defined before transferring the packets. Proactive protocols have lower latency because all the routes are maintained at all the times. Example: DSDV,WRP, FSR[2]

B. Reactive Protocols:

These types of protocols are also called as on demand routing protocols where the routes are not predefined for routing. A source node calls for the route discovery phase to determine a new route whenever a transmission is needed. This route discovery mechanism is based on flooding algorithm which employs on the technique that a node just broadcasts the packet to all of its neighbours and intermediate nodes just forward that packet to their neighbours. This is a repetitive technique until it reaches the destination. Reactive techniques have smaller routing overheads but higher latency. Example: DSR, AODV, ABR

C. Hybrid Protocols:

Hybrid protocols are the combinations of reactive and proactive protocols and takes advantages of these two protocols and as a result, routes are found quickly in the routing zone. Example: ZRP

Routing Protocols in MANETs	
Table Driven Routing Protocols	On Demand routing Protocols
Destination-Sequenced Distance Vector Routing Protocol (DSDV)	Ad-Hoc On-Demand Distance Vector Routing (AODV)
Clusterhead Gateway Switch Routing Protocol (CGSR)	Associativity Based Routing (ABR)
Wireless Routing Protocol (WRP)	Signal Stability Routing (SSR)
Global State Routing (GSR)	Dynamic Source Routing Protocol (DSR)
Hierarchical State Routing Protocol(HSR)	Temporarily Ordered Routing Algorithm (TORA)

Table 1: Categories of Routing Protocols for MANETs

III. DYNAMIC SOURCE ROUTING (DSR)

DSR is one of the reactive type of protocol. DSR is also called as on-demand protocol. It is so because the route from the source to destination is established only when required. It enhances the efficiency of the network as compared to proactive routing protocols. The other reactive routing protocols are AODV and ABR. The DSR protocol is based on the traditional Proactive DSDV protocol. In DSR protocol the source node broadcast the route request packets in the network and the intermediate nodes which is having path to the destination will reply with the route reply packets. In DSR protocol the intermediate node which further broadcast the route request packets which add its own identity in header of route request packet. When the source node start broadcasting the route request packets the header of the route request packets is empty and header will be fill by the intermediate node. The destination node will select the best path on the basis of will select best path on the basis of header value count. Katoch and Aggarwal (2013)[1] proposed that the destination wills uncast the route establishment message to the source through the intermediate nodes. The header value update approach is inefficient approach because the header value will be over flooded. The other problem in DSR protocol selects the best path on the basis of minimum hop count and highest sequence number. But in the route which is established there should be congestion. In figure 1.2 the route request packets are broadcasting and in figure 1.3 route reply packets are unicasted by the destination node.

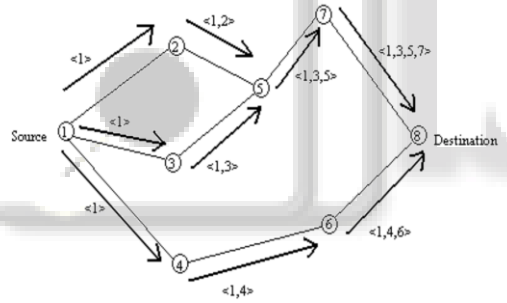

Fig. 2: Route request packets broadcasting[1]

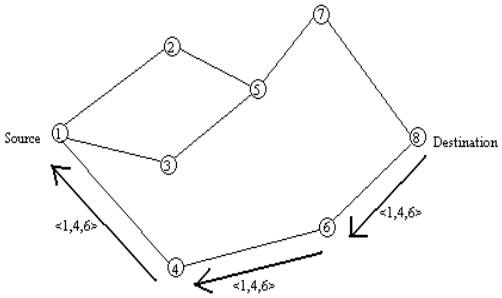

Fig. 3: Route reply packets unicast by destination[1]

A. Mechanism

Route Discovery and Route Maintenance, which are the main mechanisms of the DSR protocol, allows the discovery and maintenance of source routes in the ad hoc network's works entirely on an on-demand basis. As DSR works entirely on demand and as nodes begin to move continuously, the Routing packet overhead automatically scales to only that needed to react to changes in the route currently in use. In response to a single Route Discovery if a node learns and caches multiple routes to a destination, it can try another route if the one it uses fails. The overhead incurred by performing a new Route Discovery can be avoided when the caching of multiple routes to a destination occurs. and Mobile IP routing and supports internetworking between different types of wireless networks. [3]

B. DSR Route Discovery:

The header of the packet, which originates from a source node S to a destination node D, contains the source route, which gives the sequence of hops that the packet should traverse. A suitable source route is found normally when searching the Route Cache of routes obtained previously but if no route is found then the Route Discovery protocol is initiated to find a new route to D. Here S is the initiator and D the target. [3] Node A transmits a ROUTE REQUEST message, which is received by all the nodes in the transmission range of A. Each ROUTE REQUEST message identifies the initiator and target of the Route Discovery and also contains a unique request ID, determined by the initiator of the REQUEST. Each ROUTE REQUEST also contains a record listing the address of each intermediate node through which this particular copy of the ROUTE REQUEST message has been forwarded. The initiator of the Route Discovery initializes the route record to an empty list. [3] When the target node receives the ROUTE REQUEST message, it returns a ROUTE REPLY message to the ROUTE Discovery initiator with a copy of the accumulated route record from the ROUTE REQUEST. This route is cached in the Route Cache when the initiator receives the ROUTE REPLY and is used in sending subsequent packets to this destination. When the target node finds a ROUTE REQUEST message from the same initiator bearing the same request ID or if it finds its own address is already listed in the route record of the ROUTE REQUEST message, it discards the REQUEST.

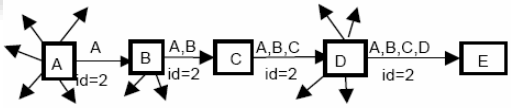

Fig. 4: Node A is the initiator and Node E is the target[3]

If the target node does not find the ROUTE REQUEST message from the initiator, then it appends its address to the route record in the ROUTE REQUEST message and propagates it by transmitting it as a local broadcast packet. When Route Discovery is initiated the copy of the original packet is saved in a local buffer called Send Buffer. The Send Buffer contains copies of each packet that cannot be transmitted by the sending node. The packets are kept until a source route is available or a timeout or Send Buffer overflow occurs. As long as a packet is in the Send Buffer, the node should initiate new Route Discovery until time out occurs or overflow of Buffer occurs. An exponential Back off algorithm is designed to limit the rate at which new ROUTE Discoveries may be initiated by any node for the same target. [3]

C. DSR Route Maintenance:

When a packet with a source route is forwarded, each node in the source route makes sure that the packet has been received by the next hop in the source route. The confirmation of receipt will be received only by re-transmitting the packet for a number of times. [3] Node A is the originator of a packet to the desired destination E. The

packet has a source route through intermediate nodes B, C and D. Node A is responsible for receipt of the packet at B, node B at C, node C at D and node D at E. Node B confirms receipt of packet at C by overhearing C transmit the packet to forward it to D. The confirmation of acknowledgement is done by passive acknowledgements or as link-layer mechanisms such as option in MAC protocol. The node receiving the packet can return a DSR specific software acknowledgement if neither of the acknowledgements is available. This is done by setting up a bit in the packet's header and then requesting a DSR specific software acknowledgement by the node transmitting the packet. When a node is unable to deliver a packet to the next node then the node sends a ROUTE ERROR message to the original sender of the packet. The broken link is then removed from the cache by the originator of the packet and retransmissions to the same destination are done by upper layer protocols like TCP. [3]

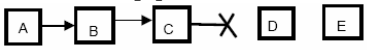

Fig. 5: Node C is unable to forward a packet from A to E over the next node D[3]

Route maintenance is also carried out also by both ROUTE REQUEST and ROUTE REPLY packets, when they traverse form each node the data from the option header of these packets which contain the link information of the nodes are updated in the nodes route cache.

D. Example of DSR

In the example given below we can see the Route Discovery and Route Reply process. N1 is the source and N8 is the destination. N1 will broadcast its message to all its neighbouring nodes that is to N2 and N3. N2 and N3 will do the same till it reaches the destination. The shortest path among them is considered. Here in the example below we can see that N5 is having the incoming paths of N1-N2 and N1-N3-N4 and it chooses N1-N2 because it is the shortest one. Similarly all the nodes will perform. At last the N1-N2-N5 will be choosen for the transmission. The destination will reply back with that node with N1-N2-N5-N8.

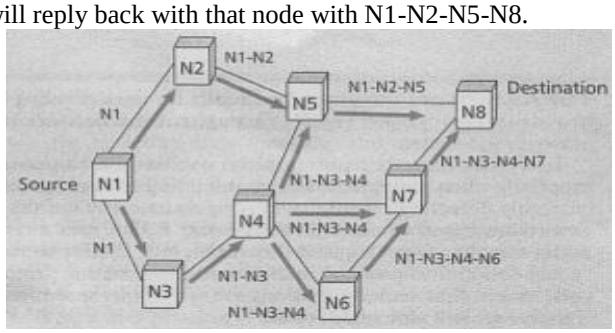

Fig. 6: Route Discovery

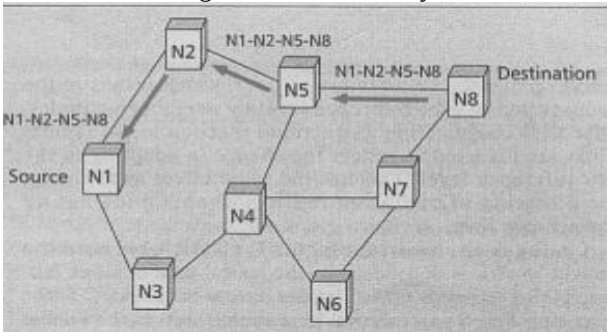

Fig. 7: Route Reply

E. Advantages of DSR

- Routes maintained only between nodes who need to communicate that reduces overhead of route maintenance
- Route caching can further reduce route discovery overhead
- A single route discovery may yield many routes to the destination, due to intermediate nodes replying from local caches

F. Disadvantages of DSR

- Packet header size grows with route length due to source routing
- No repair of broken link
- Congestion

IV. DESTINATION SEQUENCED DISTANCE VECTOR ROUTING (DSDV)

Destination-Sequenced Distance vector Routing Protocol is a table-driven routing scheme for ad-hoc mobile networks based on the Bellman-Ford algorithm. The main objective behind the designing of DSDV is to maintain simplicity and to avoid loop formation. To communicate with each other, each node has its routing tables that are stored at each node of the network. The routing table for each and every node consists of a list of all available nodes, their next hop to the destination, their metric and a sequence number which is generated by the destination node. To distinguish stale routes from new ones, the sequence number is used and thus avoid loop formation. To maintain consistency in dynamically varying topology, the stations periodically transmit their routing tables to their immediate neighbour's. If a significant change has occurred in its table from the last update sent then a station also transmit its routing table. So, the update is both time-driven and event-driven. The routing table updates can be sent in two ways: a "full dump" or an "incremental" update.

A. Congestion in DSR

One of the important restrictions of wireless ad-hoc network is Congestion. It affects the performance of the whole network. Congestion is caused because of routing and it has been detected by congestion control. There is a longer delay and packet loss while dealing with congestion also it requires significant overhead if the new route is needed. Congestion is done due to the queue overflow resulting in the loss of the data also.

Based on hop counts and sequence numbers the route have been established. The best path is that which is having minimum hop counts and higher sequence number. The sequence number tells the freshness of the route. The route will be having congestion but minimum congestion route should be selected. The queue size and current number of packets in their queue should be presented before route establishment. The nodes which is having higher queue size and less number of packets in their queue is selected as best node for data transfer. It shows that it will result in better throughput and less delay. Also packet loss will be minimum.

B. Congestion Control Techniques

Congestion detection and recovery:

- Warning bit
- Choke packets
- Load shedding
- Congestion Avoidance:
- Random early discard
- Traffic shaping

1) Warning bit:

A special bit in the packet header is set by the router to warn the source when congestion is detected. The bit is copied and piggy-backed on the ACK and sent to the sender. The sender monitors the number of ACK packets it receives with the warning bit set and adjusts its transmission rate accordingly.

2) Choke Packets:

A more direct way of telling the source to slow down. A choke packet is a control packet generated at a congested node and transmitted to restrict traffic flow. The source, on receiving the choke packet must reduce its transmission rate by a certain percentage. An example of a choke packet is the ICMP Source Quench Packet.

3) Hop-By-Hop Choke Packets:

Over long distances or at high speeds choke packets are not very effective. A more efficient method is to send to choke packets hop-by-hop. This requires each hop to reduce its transmission even before the choke packet arrive at the source.

4) Load Shedding:

When buffers become full, routers simply discard packets. Which packet is chosen to be the victim depends on the application and on the error strategy used in the data link layer. For a file transfer, for, e.g. cannot discard older packets since this will cause a gap in the received data. For real-time voice or video it is probably better to throw away old data and keep new packets. Get the application to mark packets with discard priority

5) Random Early Discard:

This is a proactive approach in which the router discards one or more packets before the buffer becomes completely full. Each time a packet arrives, the RED algorithm computes the average queue length, avg. If avg is lower than some lower threshold, congestion is assumed to be minimal or non-existent and the packet is queued. If avg is greater than some upper threshold, congestion is assumed to be serious and the packet is discarded. If avg is between the two thresholds, this might indicate the onset of congestion. The probability of congestion is then calculated.

6) Traffic Shaping:

Another method of congestion control is to "shape" the traffic before it enters the network. Traffic shaping controls the rate at which packets are sent. Used in ATM and in Integrated Services networks. At connection set-up time, the sender and carrier negotiate a traffic pattern (shape). Two traffic shaping algorithms are: (1)Leaky Bucket(2)Token Bucket

V. LITERATURE SURVEY

A. Simple Flow Counting Algorithm

Sharma and Bhardwaj(2013)[4] evaluated the effects of congestion control using OTcl. He demonstrated a simple flow counting algorithm. He added that by considering the routing and flow control, better performance and better congestion control is achieved. In his paper he considered two parameters that is varying queue length and number of sender increased.

B. Warmhole Attack Algorithm

Warmhole attack is one of the attack in DSR. It establishes private channel between the nodes and the attacker records the information. Zhang, Jiao and Zheng(2010)[5] proposed an algorithm to prevent this attack. In which some modifications have been made in DSR so that attacker is not able to attack the channel.

C. Modified Dynamic Source Routing Protocol

A black hole attack refers to an attack by malicious nodes, which forcibly acquires the route from a source to destination by falsely advertising shortest hop count to reach the destination node. Chavan, Choudhari, and Ghatage[6] proposed a Modified Dynamic Source Routing Protocol (MDSR) to detect and prevent selective black hole attack. Selective black hole attack is a special kind of black hole attack where malicious nodes drop the data packets selectively.

D. Adaptive Dynamic Source Routing

The congestion is carried out on the basis of battery level. For knowing the battery level energy level is to be calculated. And it should be between 10 to 100% and queue length should be less than 50.Average throughput, average jitter and average end-to-end delay are to be calculated. Valarmathi and Chandrasekaran (2010)[2] invoked the multi-path routing whenever threshold value is exceeded. This exceeds in large decrease of end-to-end delay by distributing traffic along multi-path.

E. Secured Dynamic Source Routing Protocol

SDSR protocol whose novelty is the trust key based on time as the additional security aspect of transferring data through trusted group nodes. Comparative analysis was proposed by Lavanya and Jeyakumar(2011)[7] to evaluate the routing performance of new proposed routing protocol SDSR with existing routing protocols namely, AODV, DSR, ZRP based on CBR traffic in terms of measuring average jitter, throughput & delay by varying the density of the network, that is the number of nodes.

F. Multipath Dynamic Source Routing Protocol

In ad hoc networks mobile devices are battery operated and the battery technology has not been improving rapidly. Therefore power consumption is likely to remain an issue in Mobile Ad-hoc Network Routing Protocols. Conventional routing protocols do not consider the power budget where the routes between nodes are built by the shortest path routing algorithms, the most popular of which are the Multipath Dynamic Source Routing Protocols. When the same algorithm is used in MANETs it may lead to a quick depletion of the energy of a few nodes because Multipath Dynamic Source Routing Protocols used more than one path for the same transmission of packets. These multiple paths allow load balancing and faster delivery. So Singh and Kumar(2013)[8] proposed an efficient algorithm, which maximizes the network lifetime by minimizing the power consumption during the source to destination route

establishment in Multipath Dynamic Source Routing Protocols.

G. Destination Sequence Distance Vector

Feng, Cai, Hu and Yang(2009)[9] proposed DSDV as a table-driven protocol and it is similar to the protocol DV (Distance Vector) of the wired routing, in which each node maintains a routing table which contains route information among nodes in the whole network. Messages could be delivered efficiently to the destination and all the mobile nodes maintains the routing table which contains all the available destinations.

H. Adhoc on Demand Distance Vector

AODV is an on-demand routing protocol. It does hop-by-hop routing. It supports unicasting and multicasting. Route discovery and route maintenance are the two major components in AODV. Before sending the packets forward it will reply back to the previous node.[2]

Parameter	DSDV	AODV	DSR
Protocols	Proactive	Reactive	Reactive
Routing	Hop-by-hop	Hop-by-hop	Source
Average Throughput	Low	Medium	High
Average Delay Time	Low	Medium	Medium
Packet Loss	High	Medium	Low
Overload, Congestion	High	Low	Low

Table 2: Comparison of different protocols

VI. IMPLEMENTATION

A. Network Simulator – ns2

Ns2 is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing and multicast protocols over wired and wireless networks. It consists of two simulation tools. The network simulator (ns) contains all commonly used IP protocols. The network animator (nam) is use to visualize the simulations. Ns2 fully simulates a layered network from the physical radio transmission channel to high-level applications.

Ns2 is an object-oriented simulator written in C++ and OTcl. The simulator supports a class hierarchy in C++ and a similar class hierarchy within the OTcl interpreter. There is a one-to-one correspondence between a class in the interpreted hierarchy and one in the compile hierarchy. The reason to use two different programming languages is that OTcl is suitable for the programs and configurations that demand frequent and fast change while C++ is suitable for the programs that have high demand in speed. Ns2 is highly extensible. It not only supports most commonly used IP protocols but also allows the users to extend or implement their own protocols. . It also provides powerful trace functionalities, which are very important in our project since various information need to be logged for analysis.

B. Simulation Environment and Implementation Outcome

In this section, we present our simulation efforts to evaluate our observations that compare the performance of the DSR routing using different topology. DSR and DSDV are also compared in terms of throughput. The simulation parameters are as follows:

Simulator	NS 2.35
Channel Type	Wireless Channel
MAC Layer	IEEE 802.11
Number of Nodes	20
Routing Protocol	DSR,DSDV

Table 3: Parameters

Transmission between nodes 0 to node 19 in DSR are shown below:

Firstly, it will broadcast the messages to all the neighbouring nodes. Till the destination is reached it will perform the same Shown in figure 1.8 and figure 1.9 the nodes broadcasting till the destination is reached.

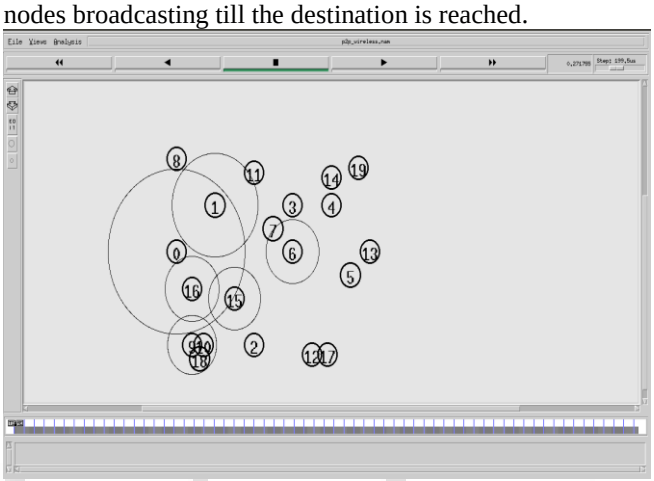

Fig. 8: Broadcasting to the neighbouring nodes

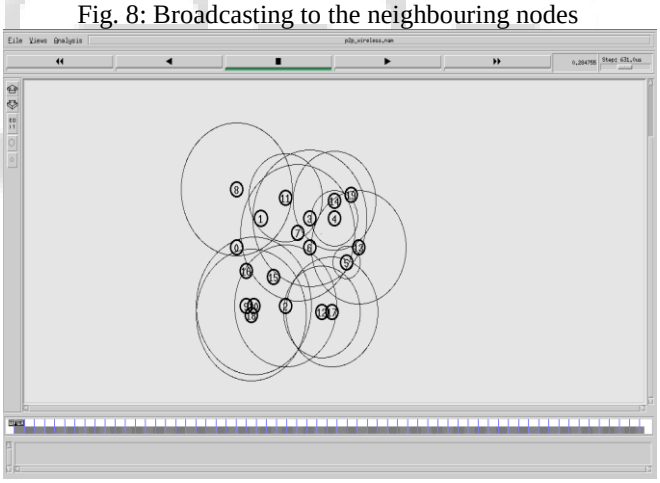

Fig. 9: Broadcasting till it reach the destination node

The average Some Packets are dropped due to congestion taking place. In the figure 1.10 we can see that the node 1 ps dropping some packets.

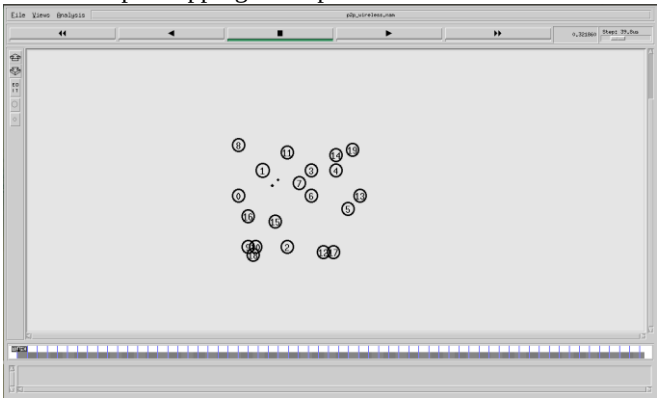

Fig. 10: Packet loss due to congestion

Now it selects the path for the transmission and transmits the data.

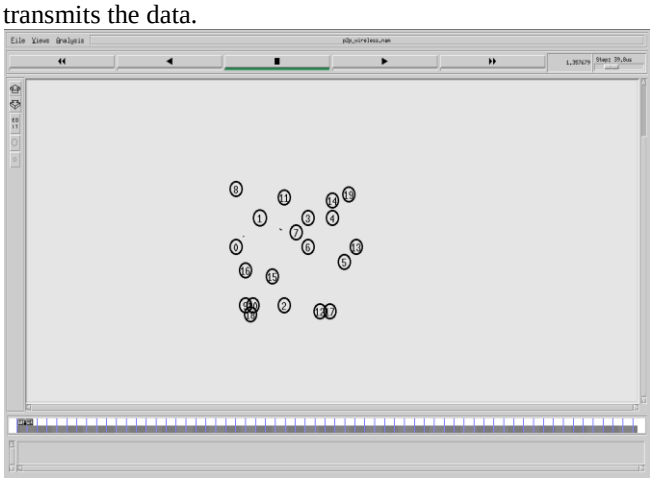

Fig. 11: Transmission from node 0 to 7

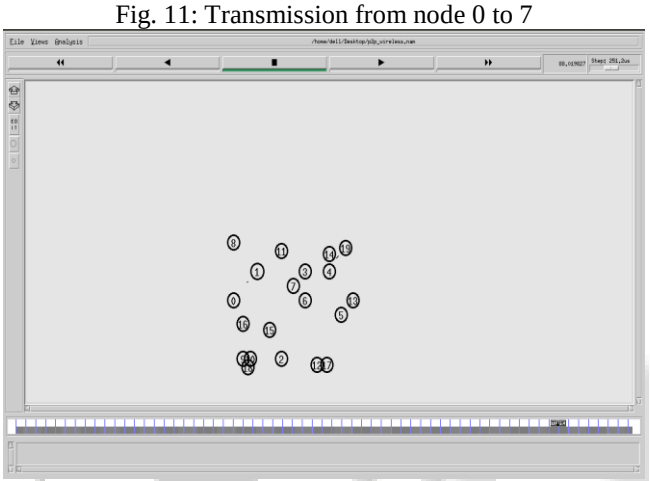

Fig. 12: Transmission of nodes till the destination node 19

Below is the graph of DSR protocol in terms of Time versus Throughput. DSR stores source routes it has learned, it also costs little time and bandwidth to maintain the altered routes. As a result of such concentration on packets delivery, DSR enjoys a decent average throughput compared with others.

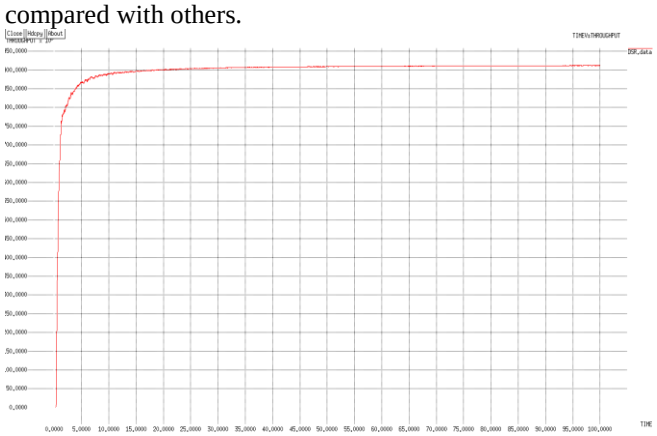

Fig. 13: Graph of Time versus Throughput in DSR Protocol

Transmission between node 0 to node 19 in DSDV are shown below:

Now the transmission of DSDV protocol is shown below. In DSDV protocol the tables are updated of every nodes and then the transmission takes place. It chooses the shortest path for the transmission.

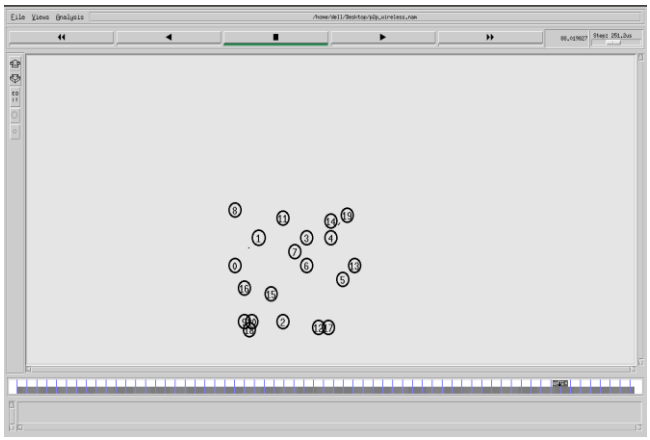

Fig. 14: Transmission of nodes till destination in DSDV

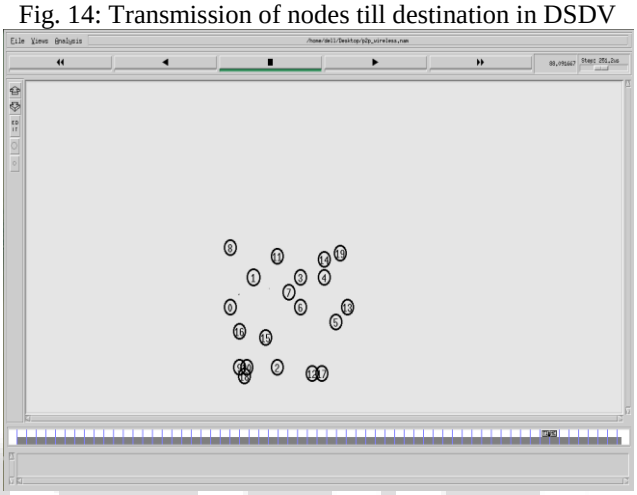

Fig. 15: Transmission of nodes from destination in DSDV

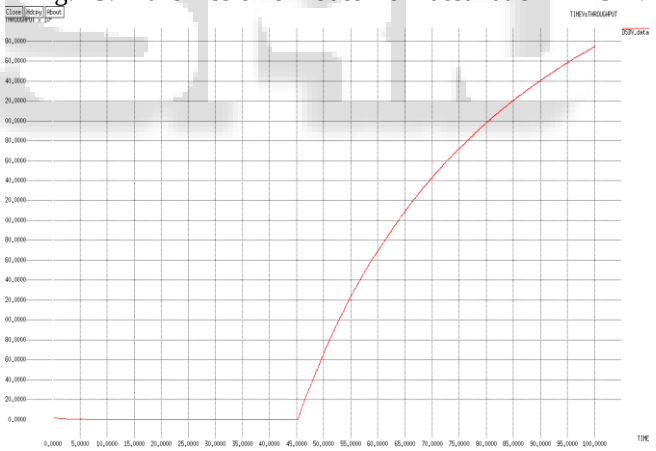

Fig. 16: Graph of Time Vs Throughput of DSDV Protocol

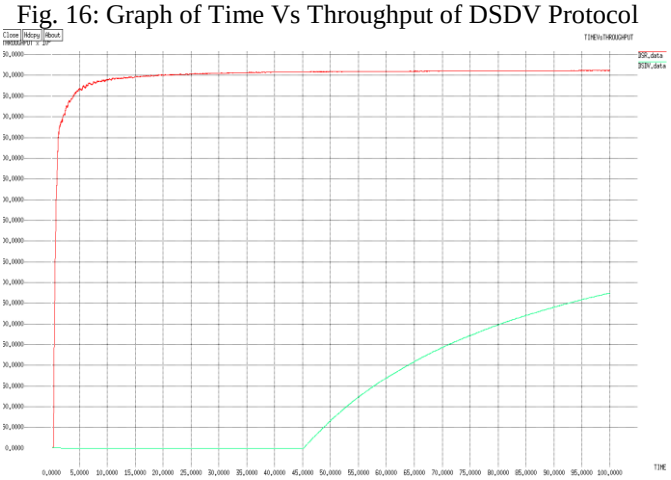

Fig 1.17: Comparison of DSR and DSDV Protocol

From the above graph we conclude that DSDV requires extra time to set up routing tables before delivering packets. So the average throughput turn out to be less than that of DSR.

VII. CONCLUSION AND FUTURE WORK

DSR protocol is an efficient routing protocol. Routes are properly discovered and maintained. It chooses its shortest path for delivering data. DSR is better than DSDV in terms of throughput as DSDV requires more time to set up the routing table before delivering packets.

In future, simulation of DSDV and DSR protocol are performed in a large scale network. The comparison of DSV and DSDR protocol on different parameters like packet ratio delivery, energy, end-to-end time delay.

REFERENCES

[1] Katoch, S., and Aggarwal, R., "Enhancement in DSR Protocol for Load Balancing and Congestion control," Global Journal of Computer Science and Technology Network,Web & Security, vol. 13, Issue 7, Version 1.0, 2013.
[2] Sravya. V1., Nagaraju. A2., and Pavani. K3. "Performance Evaluation of IEEE 802.11 with DSDV, DSR, AODV Routing Protocols in MANETs," International Journal of Engineering and Science, vol. 2, Issue 1, 2013.
[3] Ragunath V., "Implementation of DSR Protocol in NS2 simulator," University of Bonn,Informatik department 4.
[4] Sharma, G. and Bhardwaj, A.K., "Congestion Control in Adhoc Network," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, Issue 6, 2013.
[5] Valarmathi, A. and Chandrasekaran, R.M., "Congestion Aware and Adaptive Dynamic Source Routing Algorithm with Load Balancing in MANETS," International Journal of Computer Applications (0975 – 8887), vol. 8, No.5, 2010.
[6] Chavan, R.V., Choudhari, M.S. and Ghatage, R.A., "Survey Enhancement of Modified DSR protocol For Removal and Detection of Selective Black Hole Attack n MANET," IJARCET, vol. 33, Issue 10, 2014.
[7] Lavanya, G. and Ebenezer, A.J., "An Enhanced Secured Dynamic Source Routing Protocol for MANETS," International Journal of Soft Computing and Engineering (IJSCE) ISSN:2231-2307, vol. X, Issue 4, 2011.
[8] Zhang, D., Jiao, W. and Zheng, J., "Research and Improvement of DSR Protocol in AdHoc Network,"2nd International Conference on Industrial & Information System, 2010.
[9] Feng, Q., Cai, Z., Yang, J. and Hu, X., "A Performance comparison of the Ad Hoc Network Protocols," IEEE DOI 10.1109/WCSE.2009.816, 2009.

