Volume 4, Issue 9, September 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Evaluation of DSR Routing Protocol Embedded With a Code to Improve the Performance of Movement of Nodes in MANET Using NS-2

Anuj Kumar Singh
Research Scholar, GRDIMT
Dehradun, India

Anurag Kumar
Asst.Professor, GRDIMT
Dehradun, India

Abstract- Dynamic source routing protocol is a simple routing protocol designed for multi hop wireless ad hoc mobile nodes. Routes in DSR protocol is decided by each nodes itself rather than routing table.

Each node acquires the address of each device from source to destination. All the routing information is maintained by mobile nodes.

But due to some Malicious code routing information is lost which leads to performance degradation. In this paper we have tried to embedded a code in the DSR routing protocol through which we can improve the performance of movements of node in a network. Through this code we can suppress the effect of malicious code in finding the route in multi hop wireless ad hoc mobile nodes.

For evaluation we have use NS-2.34 simulation environment. Through simulation we calculated the performance and throughput with malicious code of DSR routing protocol.

Keywords: MANET, Routing Protocols, Network simulator NS-2.34, Malicious Node.

I. INTRODUCTION

MANETs is an IEEE 802.11 framework. It consists of wireless mobile nodes that form a temporary network without the aid fixed infrastructure or central administration and also known as self configuring network of mobile node connected by wireless links [1] and [3]. Nodes can communicates directly to other nodes within their transmission range. Nodes outside the transmission range are communicated via intermediate nodes such that it forms a multi-hop scenario. In multi-hop transmission, a packet is forwarded from one node to another, until it reaches the destination with the help of using routing protocol. For proper functioning of the network cooperation between nodes is required [1], [2] and [5]. It is also referred as an infrastructure less network because the mobile nodes in the network dynamically locate paths among themselves to transfer packets provisionally. Due to the dynamic network topology in ad hoc network nodes are exchanging plenty of routing packets for creating communication which intern increase network overhead and also increase collision in network [2]. Figure 1.1 shows the general Architecture diagram for the mobile Ad hoc network.

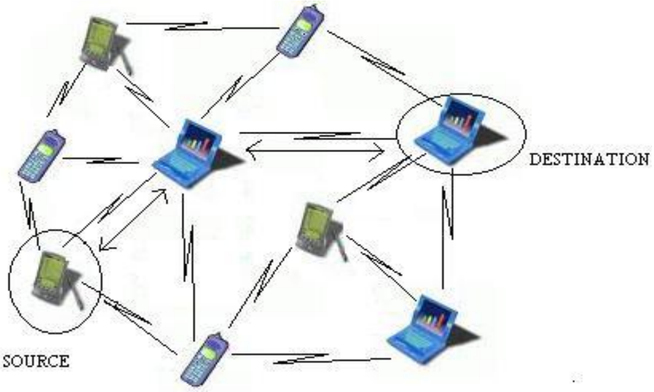

Figure 1.1: General Mobile Ad hoc Network Architecture

In MANET each node behaves like a terminal as well as a router and devices are mobile nodes which provide the functionality required to connect users allowing them to exchange information in an environment with no pre-established infrastructure. The terminals are generally mobile and change the network topology dynamically by their mobility. MANETs are capable of handling topology changes due to mobility, malfunctioning nodes and links through network reconfigurations. MANET topology and location changes rapidly and unpredictably, therefore the network needs routing protocols that can respond to the topological changes instantly [5].Routing protocols for MANET must be adaptive and capable of maintaining routes despite network topology changes [6]. MANETs facilitates communication among the mobile users in situations-military or civil emergency where fixed infrastructure is infeasible.

II. AN OVERVIEW OF DYNAMIC SOURCE ROUTING(DSR) PROTOCOL

DSR is a reactive routing protocol which is able to manage a MANET without using periodic table update message like table driven routing protocols do [2] and [5]. The Dynamic Source Routing (DSR) protocol is a simple and robust routing protocol designed for use in multi-hop wireless ad-hoc networks of mobile nodes. It is an on-demand routing protocol without any periodic routing advertisement messages. Through DSR protocol hardly provides any QoS support, multicasting and security, it can easily adapts to changes like host movement without requiring considerable protocol overheads. DSR can switch easily between the extreme situations where movement of hosts is quick and frequent i.e. where flooding may be the best strategy, as well as infrequent movements which are almost static i.e. where conventional routing protocols are most suitable. DSR was specifically designed for use in multi hop wireless ad hoc networks and DSR allows the network to be completely self-organizing and self-configuring [7] and [8] without the need for any existing network infrastructure or administration. Ad hoc protocol allows the network to be completely self-organizing and self-configuring which means that there is no need for an existing network infrastructure or administration [2], [3] and [5]. For restricting the bandwidth, the process to find a path is only executed when a path is required by node (on-demand routing). In DSR the Sender (source, initiator) determines the whole path from the source to the destination node (source routing) and deposits the address of the intermediate node of the route in the packets. DSR was developed for MANET's with a small diameter between 5 and 10 hops and the node should only move around at a moderate speed. DSR is based on the link-state-algorithms which mean that each node is capable to save the best way to a destination [1] and [9]. Also if a change appears in the network topology, then the whole network will get this information by flooding. DSR has increased traffic overhead by containing complete routing information into each data packet, which degrades its routing performance. DSR is only applicable to a relatively small amount of nodes, less than 100. Otherwise, managing the source routes to every node may become problematic.

III. RELATED WORK

Routing is the act of moving information from a source to a destination in an internetwork [5]. During the transfer of information at least one intermediate node within the internetwork is encountered. Mainly two activities are concerned in this concept: transferring the packets through an internetwork and shaping optimal routing paths. The transferring of packets through an internetwork is known as packet switching which is straight forward, and the path determination could be very complex. Routing protocols use a number of metrics as a standard measurement to analyze the best path for routing the packets to its destination that could be number of hops, which are used by the routing algorithm to determine the optimal path for the packet to its destination. The process of path determination is that, routing algorithms find out and maintain routing tables, which contain the total route information for the packet. The information of route varies from one routing algorithm to another. The routing table's are filled with entries in the routing table are ip address prefix and the next hop [4].

In MANET over the inimical node we evaluated the performance. The inimical node of DSR attacks on the Ad-hoc network which degrades the performance of routing algorithm. So our research is based on evaluation of result to control high effort over change of code with the inimical node in DSR protocol and also with the normal DSR code.

By the result analysis inimical node have harmful effect on network. The speed of network play important role to reduce effects of these nodes. In order to evaluate the feasibility and effectiveness we evaluate the performance on default associated code with ns2.34.

1) Normal DSR Code: This is normal installed code given in the network simulator.
2) Inimical DSR Code: We implemented an inimical node for evaluation of new performance in the given normal DSR code through use of route request function in the protocol.
3) Improved DSR Code: In this the DSR code with inimical node and improvement on forward function of DSR code to improve the performance and remedy of inimical node.

Proposed Improved Dynamic source routing protocol Algorithm

Step-1 Test the selfish and inimical node by broadcast request to neighboring nodes in improved Dynamic source routing protocol code file which is Dsragent.cc.

Step-2 Test whether the node in improved code of dynamic source routing protocol is inimical or not

Step-3 Forward packets or given request and reply to next node otherwise drop data packets when node is selfish and inimical.

Step-4 Else insert to route information of RREQ (Route request) and forward all request, reply and data packets.

Step-5 On the particular selfish and inimical nodes which is take part improved Dynamic source routing Protocol its effect being reflected in performance on results

Function used to forward the packet to improve performance

1) After receiving the RREQ(route request) drop the packet otherwise forward the packet as given function. SendOutPacketWithRoute (p,false, srh->route_reply())
2) After receiving the RREP(route reply) drop the packet otherwise forward the packet as given function to improve the performance over inimical DSR code.

SendOutPacketWithRoute (p,false,srh->route_reply())

IV. SIMULATION SETUP

The Network Simulator Version 2.34 is a deterministic discrete event network simulator, initiated at the Lawrence Berkeley National Laboratory (LBNL) [10] through the DARPA funded Virtual Inter Network Testbed (VINT) project. NS-2 is used in the simulation of routing protocols, and is heavily used in ad-hoc networking research.

This section describes the various scenarios for which simulation was performed on the base of random waypoint mobility model with the varying nodes and varying pause time with fix speed of the network. All scenarios were tested separately against inimical dynamic source routing protocol and improved source routing protocol and different graphs were obtained after trace analysis.

Table 1.1: Simulation Parameters for Varying nodes and pause time

Protocols	Dynamic source routing
Simulation Area	1200 *800
Simulation Time	200 sec
No of Nodes	10, 20, 30, 40 ,50
Mobility Model	Random way point
Maximum Speed	20 m/sec
Pause Time	10, 20, 30, 40, 50 sec
Type of Traffic	CBR
Size of Payload	512 bytes
Packet Rate	10 packets/sec
Maximum Connection	20

V. RESULT DISCUSSION

Varying nodes and Pause time

Figure 1.2 tells about the Packet Delivery Ratio. We analyzed the results by AWK scripting file in the network simulator to calculation of the performance.

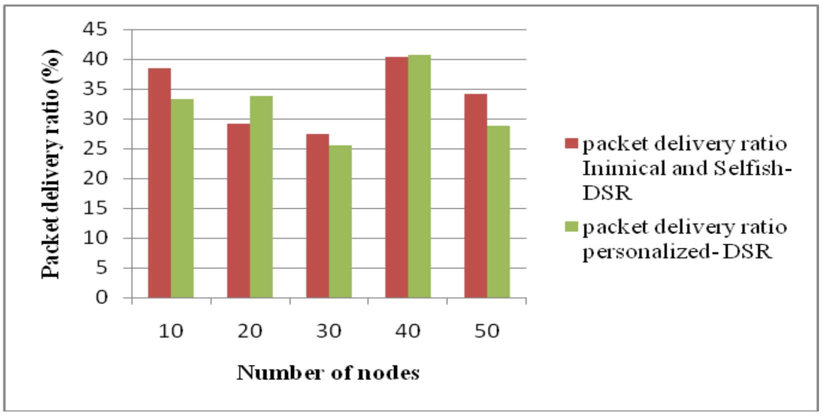

Figure 1.2: PDR with varying nodes and pause time

So by simulation result we can say that packet delivery ratio of selfish and inimical nodes dynamic source routing has low performances than improved dynamic source routing protocol on the default dynamic source routing protocol. When we implemented with inimical node the PDR reduces. It is also seen that on applying Improved DSR performance becomes slight better.

Figure 1.3 shows the average end-end delay, as per the variation in pause time and number of nodes, it is noticed that improved dynamic source routing protocol performs better than selfish and inimical dynamic source routing.

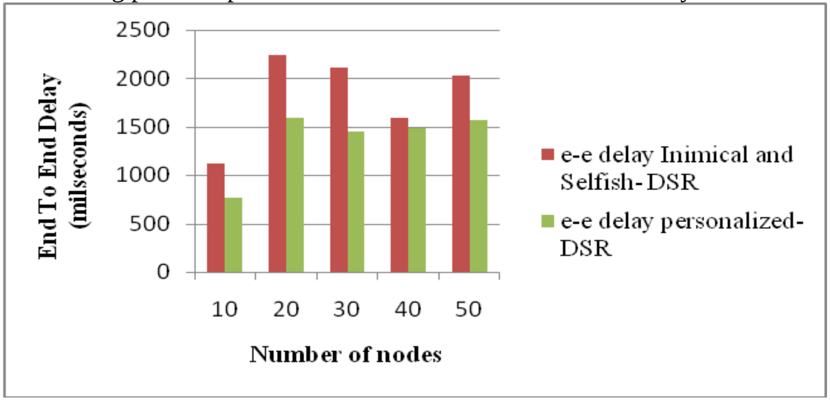

Figure 1.3: end to end delay with varying nodes and pause time

Figure 1.4 shows the result for the Packet Loss, Improved dynamic source routing protocol packet loss is minimum in all the cases as compared to selfish and inimical nodes dynamic source routing protocol by varying pause time and number of nodes.

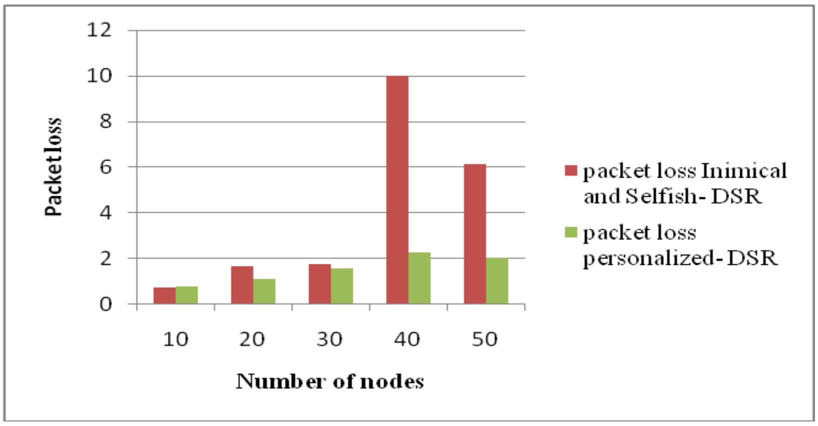

Figure 1.4: Packet Loss with varying nodes and pause time

Figure 1.5 shows the result of Routing Overhead in the network, the performance of improved dynamic source routing protocol is much better when compared with selfish and inimical misbehaviour on the default dynamic source routing protocol.

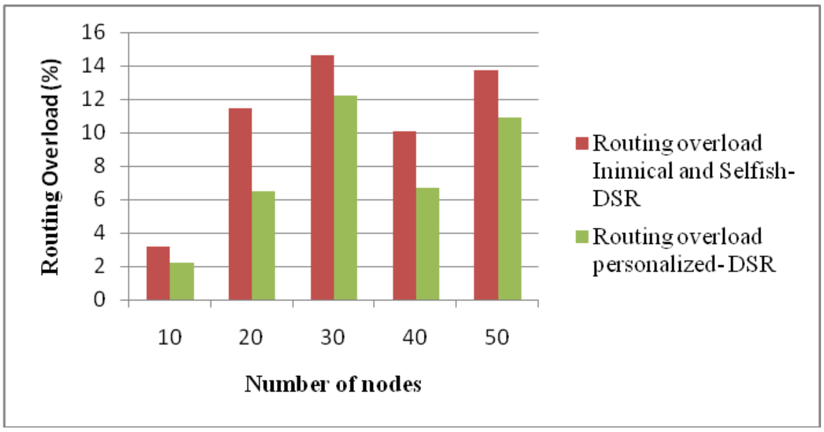

Figure 1.5: Routing Overload with varying nodes and pause time

Figure 1.6 shows the result of throughput, as according to varying number of nodes and varying pause time with fix maximum connection and data rate.

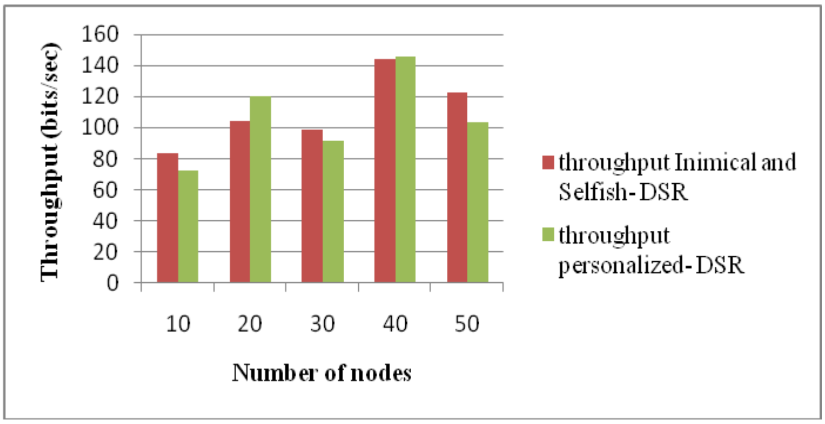

Figure 1.6: Throughput with varying nodes and pause time

The throughput of personalized dynamic source routing protocol is better compared to the selfish and inimical nodes dynamic source routing protocol when nodes increase.

Varying Speed of network

Figure 1.7 shows simulation result that say packet delivery ratio of normal DSR is better than others. But when DSR implemented with inimical node the PDR reduces. It is also seen that on applying Improved DSR performance becomes slight better.

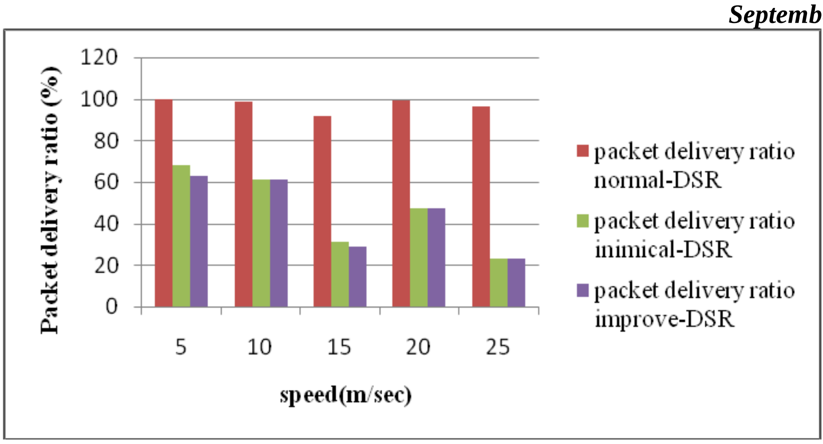

Figure 1.7: PDR with varying speed

As per the variation in pause time, simulation time and number of nodes, it is noticed that Improved DSR code performs better than inimical DSR (Figure 1.8).

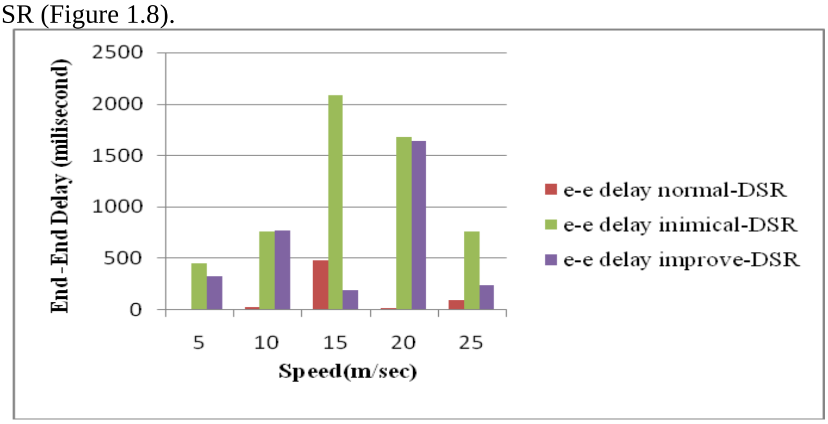

Figure 1.8: End to end delay with varying speed

In Figure 1.9 improved DSR packet loss is minimum in all the cases as compared to normal DSR. Normal DSR has more packet loss over varying speed as compared to Improved DSR by varying pause time and number of nodes also.

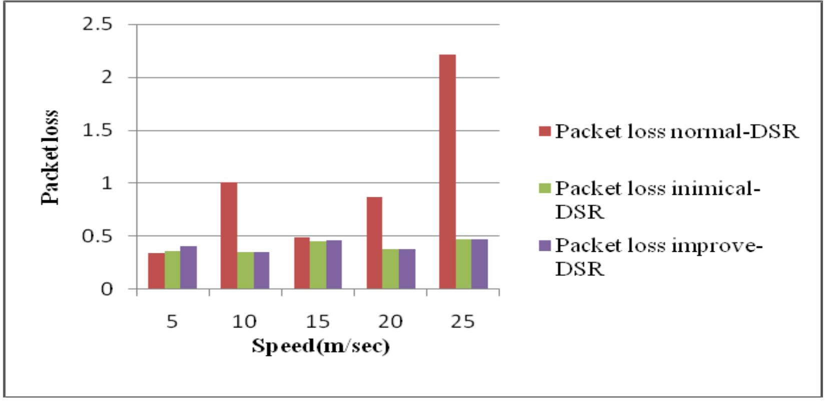

Figure 1.9: Packet Loss with varying speed

Figure 1.10 shows the performance of Improved DSR is much better when implemented with inimical or malicious node.

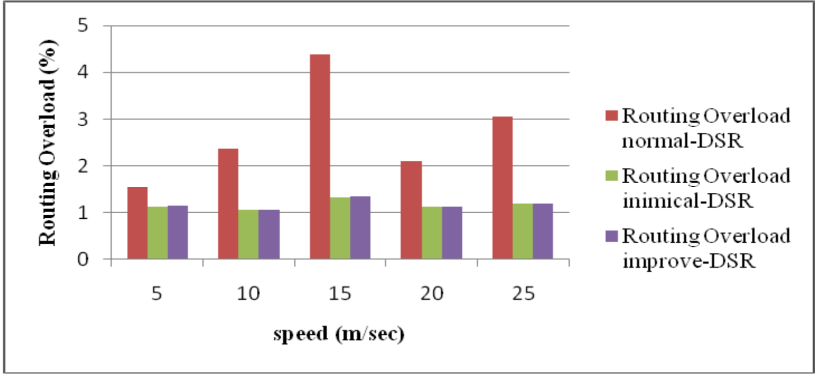

Figure 1.10: Routing Overload with varying speed

In Figure 1.11 as according to number of nodes and varying speed with fix pause time.

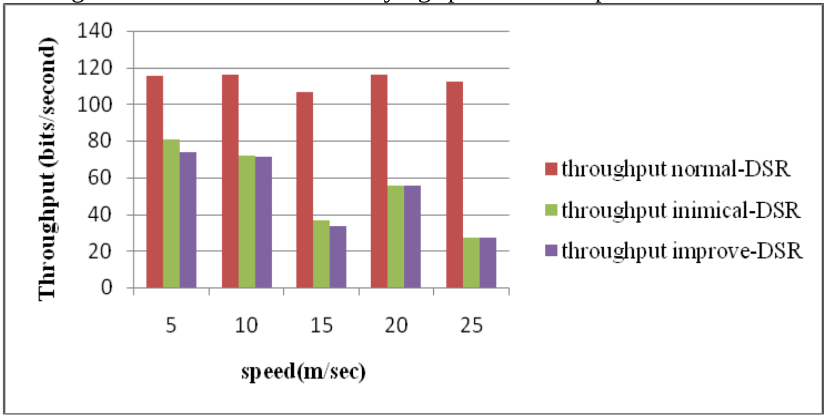

Figure 1.11: Throughput with varying speed

The throughput of normal DSR is way better compared to the inimical or Improved DSR. But when the node starts dropping packets then improve DSR code is better than inimical DSR.

VI. CONCLUSION

The inimical and selfish nodes attacks, which disrupts a packet or do not forward the packet to the destination by inimical node behavior. So the research is based on evaluation of result to control high affect over change of code with the inimical nodes in dynamic source routing protocol and also with the improved dynamic source routing protocol code. In this research we changed the normal dynamic source routing protocol which is installed code given in the network simulator with the new code with misbehavior nodes. After changes we implemented and analyzed the performance of dynamic source routing protocol over the selfish and inimical nodes which degraded the peroformance of default dynamic source routing protocol. For the better performance we provide solution as Improve dynamic source routing protocol on the default dynamic source routing protocol installed on the network simulator

REFERENCES

[1] G.Lavanya, A. Ebenezer jeyakumar,” An Enhanced Secured Dynamic Source Routing Protocol for MANETs”, International journal of soft computing and engineering (IJSCE) ISSN: 2231-2307,volume X,Issue-4,September 2011.

[2] H. ZAFAR, L. HASAN, A. KHATTAK, Z. MUFTI, S. JAN, “Implementation of dynamic source routing protocol in network simulator 2”,Sindh Univ. Res. Jour. (Sci. Ser.) vol.44(3) 491-496,2012.

[3] Sourav Ghosh & Chinmoy Ghorai,” Evaluating the Performance of Modified DSR in Presence of Noisy Links using QUALNET Network Simulator in MANET”, International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) ISSN No. 2248-9738 (Print) Volume-1, Issue-2, 2011.

[4] Rajendra V.Boppana, Anket Mathur,”Analysis of the Dynamic Source Routing Protocol for Ad Hoc Networks,” 2005.

[5] D.B. Johnson, D.A. Maltz, and Y. Hu, “The Dynamic Source Routing Protocol for Mobile ad-hoc Networks (DSR),” IETF Internet Draft, July 2004.

[6] Disha G. Kariya, Atul B. Kathole, Sapna R. Heda,”Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method”, International Journal of Emerging Technology and Advanced Engineering, website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 1, January 2012).

[7] Carlos de Morais Codeiro, Dharma P.Agarwal,” Mobile Ad hoc networking”, OBR Research center for Distributed and mobile computing, ECECS.

[8] George Aggelou, “Mobile Ad Hoc Networks”, 2nd edition, Mc GRAW Hill professional engineering, 2004.

[9] D. B. Jagannadha Rao1 ,Karnam Sreenu2, Parsi Kalpana,” A Study on Dynamic Source Routing Protocol for Wireless Ad Hoc Networks”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 8, October 2012

[10] NS-2, the NS Manual, Available at http://www. isi.edu/nsnam/ns/doc