IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)
ISSN(E): 2321-8843; ISSN(P): 2347-4599
Vol. 2, Issue 8, Aug 2014, 1-10

DETECTION OF SELFISH NODE IN DSR BASED MANET USING REPUTATION BASED SCHEME

SANTOSH KUMAR & SUVEG MOUDGIL

Department of Computer Science & Engineering, HEC, Jagadhri, Kurukshetra University, Kurukshetra, India

ABSTRACT

MANET is an autonomous system of mobile nodes connected by wireless links. Mobile ad hoc networks are prone to a number of security fears. To handle the selfish nodes is major issue in ad hoc network. The Dynamic Source Routing protocol is a simple and strong routing protocol designed especially for the use in wireless ad-hoc networks of mobile nodes. The use of the source routing allows packet routing to be slightly loop-free, avoid the need for up to date routing information in the intermediate nodes through which packets are forwarded and allows nodes forwarding to cache the routing information in them for their own future use. Reputation of a node can be calculated using a simple formula and a node is supposed to maintain a good reputation value to participate in route discovery process otherwise discard in route discovery. In this paper the DSR protocol based on reputation scheme is implemented to detect the selfish node and the evaluation is done through performance metrics (Packet delivery ratio, Average end to end delay) in Network Simulator.

KEYWORDS: DSR, Mobile Ad Hoc Network, Reputation DSR, Reputation/Trust, Routing, Selfish Node

INTRODUCTION

A mobile ad hoc network is an autonomous system of mobile nodes connected by wireless links. Each node operates not only as an end-system, but also as a node to forward the packets. The nodes are free to move about and organize themselves into a network. The main application of mobile ad hoc network is in emergency rescue operations and battlefields [2]. Many routing protocols have been proposed for reliable information exchange in a network.

Routing Protocols

In Mobile ad hoc network the routing is a difficult task and it is very different from routing protocols in traditional wired world. [11] some of reasons are mobile ad hoc network are frequently route updates topology changes due to failures of nodes. There are limited transmission ranges of nodes in mobile ad hoc network.

Proactive Protocols

Proactive Routing Protocols attempt to maintain consistent, up-to-date routing information between every pair of nodes in the network. In proactive routing, each node has one or more tables that contain the latest information of the routes from one node to any other node in the network. Each row has the next hop for reaching a node or subnet and the cost of this route. Various table-driven protocols differ in the way the information about a change in topology is propagated through all nodes in the network [16].

Reactive Protocols

Reactive routing protocols can considerably reduce routing transparency because they do not need to search for

and maintain the routes on which there is no data traffic [11]. Reactive routing is also known as on-demand routing. These protocols take a lazy approach to routing. They do not maintain or constantly update their route tables with the latest route topology. Reactive routing protocols establish a route to a destination when there is a demand for it.

Dynamic Source Routing

Dynamic Source Routing uses source routing to deliver packets from one node in the network to some other node. The source node adds the full path to the destination in terms of intermediate nodes in every packet [1]. This information is used by intermediate node to determine whether to accept the packet and to whom to forward it. DSR operates on two mechanisms are following

- Route Discovery
- Route Maintenance

Route discovery is used when the sender does not know the path up to the destination. In this mechanism, the sender broadcasts a route request message which contains source address, destination address, and identifier. Each intermediate node adds its address in route request message and rebroadcast it, unless it has not rebroadcast earlier. With this controlled broadcast, the route request will ultimately reach the destination. The destination then sends a unicast route reply message in reverse direction whose information is obtained from list of intermediate nodes in route request message. When the route reply packet reaches the source, it records the route contained in it and saves in its cache for the specific destination. For better performance, intermediate nodes also record this route information from the two route messages. All nodes overhearing these packets add meaningful route entries in their caches. Finally, route maintenance mechanism is used to notify source and potentially trigger new route discovery events when changes in the network topology invalidates a cached route [5].

Reputation Based Approach in MANET collects information about one entity's former behavior as experienced by others. Reputation Based approach provide solution based on trust evaluation process for a node implies significant lower energy consumption, less processing for trust level calculation. In this paper we proposed a Security framework for DSR using reputation based scheme that uses reputation with cache clearance process that not only improve the efficiency and reduce network overhead but also permit every node to participate into the route selection process for communication.

ATTACKS IN MANET

Mobile ad hoc network is highly vulnerable to attacks. Attacks are classified in two categories

Passive Attacks

Passive attacks are the attack that does not disrupt proper operation of network. Attackers snoop data exchanged in network without altering it. Requirement of confidentiality can be violated if an attacker is also able to interpret data gathered through snooping [15]. Detection of these attacks is difficult since the operation of network itself does not get affected.

Active Attacks

Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the attacks. Active attacks involve some modification of data stream or creation of false stream.

Black Hole Attack

In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it [15]. A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.

Selfish Nodes

Mobile ad hoc network is highly vulnerable to attacks. In this node is not serving as a relay to other nodes which are participating in the network. This malicious node which is not participating in network operations, use the network for its advantage to save its own resources such as power [15].

Worm Hole Attack

In a wormhole attack, an attacker receives packets at one point in the network, “tunnels” them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunnelled. This tunnel between two colluding attacks is known as a wormhole. In DSR, this attack could prevent discovery of any routes and may create a wormhole even for packet not address to itself because of broadcasting. Wormholes are hard to detect because the path that is used to pass on information is usually not part of the actual network. Wormholes are dangerous because they can do damage without even knowing the network [15].

RELATED WORK

There are many solutions in the literature which deals with misbehaving nodes using reputation mechanisms. This section explains only some of them

Sohail Abbas et al. survey and categorize reputation based schemes according to their passive and active acknowledgment monitoring techniques in multi hop networks such as mobile ad hoc networks selfish or misbehaving nodes can disrupt the whole network and severely degrade network performance [2]. Rajesh Sharma et al. They had discussed a solution on the basis of reputation method to solve routing issues raised by misbehaving nodes [1]. Renu Dalal et al. provide the different ways to achieve trust in mobile Ad-hoc Network. Providing the safe communication between mobile nodes, reorganization the position of nodes, reducing overhead, handling misbehaviour and location updates are such a difficult issues in ad-hoc network so providing trust schemes is an important in this network [3]. Santhosh Krishna B. Vet et al. The author focus on single and multiple black hole attacks. The implementations of black hole comprises active routing misbehaviour and forwarding misbehaviour & design and build our prototype over DSR and test it in Network simulator 2 in the presence of variable active black hole attacks in highly mobile and sparse networks [5]. Isaac Woungang et al. provide a novel scheme for Detecting Black hole Attacks in MANETs is introduced. The BDA-DSR protocol detects and avoids the black hole problem before the actual routing mechanism is started by using fake route request packets to catch the malicious nodes [6]. Poonam K Gar et al. They had discussed and proposed a new algorithm to find route to the destination as a weighted average of the trust value of the nodes in the route, with respect to its behavior observed by its neighboring nodes and the number of nodes in the route is calculated [9]. Sangheetaa Sukumran et al. proposed a solution for on-demand routing protocol using reputation mechanism. This approach calculates the reputation values of the nodes using simple formula. Any node is supposed to maintain a good reputation value in order to receive

network services. When a node tries to identify a route, its route request will be forwarded by the neighboring nodes only if it reputation value is higher than the threshold value i.e. this node must be in the white list. Thus a node needs to maintain a good reputation value in order to enjoy network services. A misbehaving node which is isolated has no chance of rejoining the network until the entire network is reformed. This will decrease the efficiency and effectiveness of the network, low reputation value node is not allowed to participate in a network until network is reformed. We provided a solution that uses reputation with cache clearance process that not only improve the efficiency and reduce network overhead but also permit every node to participate into the route selection process for communication. [10]

PROPOSED WORK

In this paper, we proposed an approach for increasing the efficiency of Dynamic source routing protocol using trust based route selection process. Our solution is based on the concept of behavior trust; for trust level calculation. In this Reputation value is calculated [10] using equation below.

Suppose there are 27 nodes in the mobile ad-hoc network. Each node calculates the reputation R (i, j) t for each of its neighbor j at time t.

$$R_{(i,j)t} = \frac{\sum_{Pkts=0}^{\infty} F_{pkts}}{\sum_{Pkts=0}^{\infty} S_{pkts}}$$

Where Reputation of i and j at time t is the reputation value calculated by monitoring the neighbor j directly at time t and Fpkts is the number of packets forwarded by node j and Spkts is the number of packets sent by node j.

As a result, a node with the highest reputation will get the chance to participate in communication fixed time period cache will get clear, this process refresh the reputation value of each node so that every node will get chance to participate in the communication it will increase performance and efficiency of the network

Proposed Algorithm

In reputation based monitoring module continuously monitors node behaviour and assign a reputation values to nodes based on their packet forwarding activity in the routing table.

Step 1: Each node maintains reputation values of its neighbours and other nodes that have had a transaction with it.

Step 2: Packet forwarding between two nodes depend on the mobility factor. A node observes a packet forwarded by neighbours Q. To calculates the reputation value R (P, Q) equal to the ratio of packet delivered by Q to the total number of packets sent by node P.

Step 3: A node P can obtain opinion about Q by requesting reputation value from its neighbours.

Step 4: As a result of node with reputation value is greater than threshold value can participate in route discovery process.

SIMULATION SETUP & RESULTS

Simulation Environment

Simulations are performed in NS-2 which stands for Network Simulator 2, a network simulator that provides support for simulating multi-hop wireless networks complete with physical and IEEE 802.11 MAC layer models.

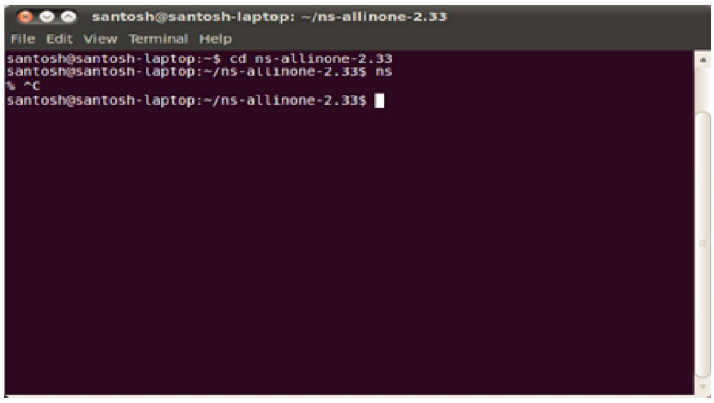

Figure 1: Simulation Environment

The mobile nodes move according to the "random waypoint" model. Each mobile node begins the simulation by remaining stationary for pause time seconds. It then selects a random destination in the defined topology area and moves to that destination at a random speed. The random speed is distributed uniformly between zero (zero not included) and some maximum speed. Upon reaching the destination, the mobile node pauses again for pause time seconds. This movement pattern is repeated for the duration of the simulation. The movement patterns are generated by CMU's 1 movement generator (setdest).

Simulation Parameters

There are two scenario's consisting of 27 nodes in which one selfish node is present in each at different locations. The parameters described in table 1 are taken for the simulation.

Table 1: Simulation Parameters

Parameter	Value
Number of Nodes	27
Traffic Sources	01
Type of Traffic	TCP
Packet Size	512
Simulation Time	20 m & 25 m
Topology Area	1200 *1200
Routing Protocol	DSR
MAC Protocol	802.11
Selfish Node	01
Mobility Patterns	Random waypoint

Scenario

There are two scenario's consisting of 27 mobile nodes. The topology is a rectangular area with 1200 m length and 1200 m width. A rectangular area was chosen in order to force the use of longer routes between nodes than would occur in a square area with equal node density. Mobile nodes respectively are TCP traffic sources.

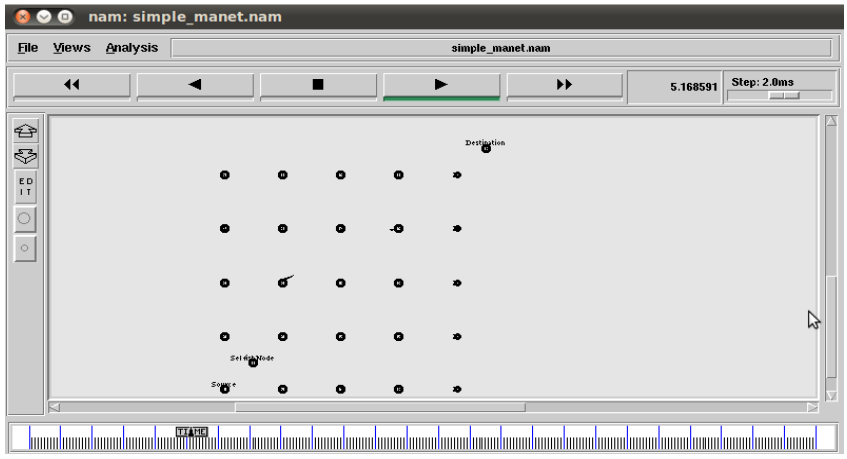

Figure 2: Node Scenario 1 with One Selfish Node

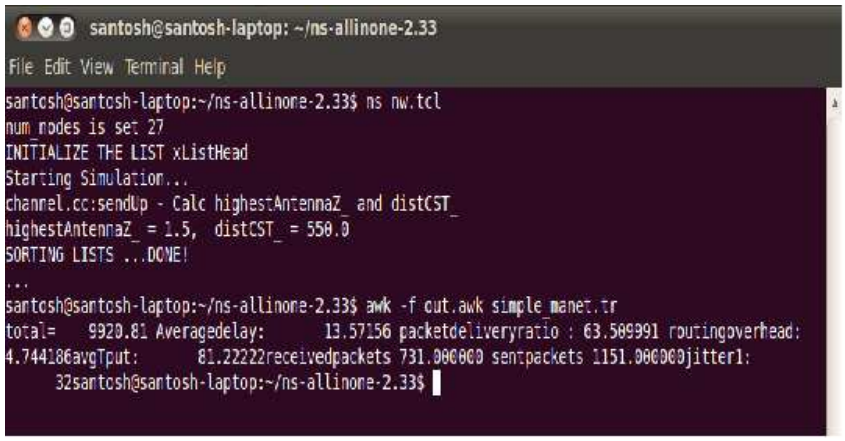

Figure 3: Parameter Results of Scenario 1

Figure 3 shows out of total 1151 packets 731 packets are received with drop of 420 packets. The Throughput is 81.22 bps.

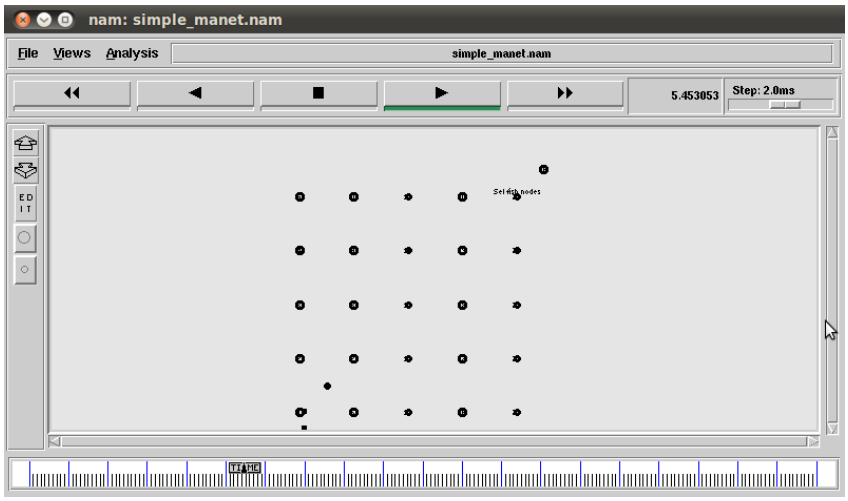

Figure 4: Node Scenario 2 with One Selfish Node

In Figure 2 & Figure 4 shows the different route selection process for communication.

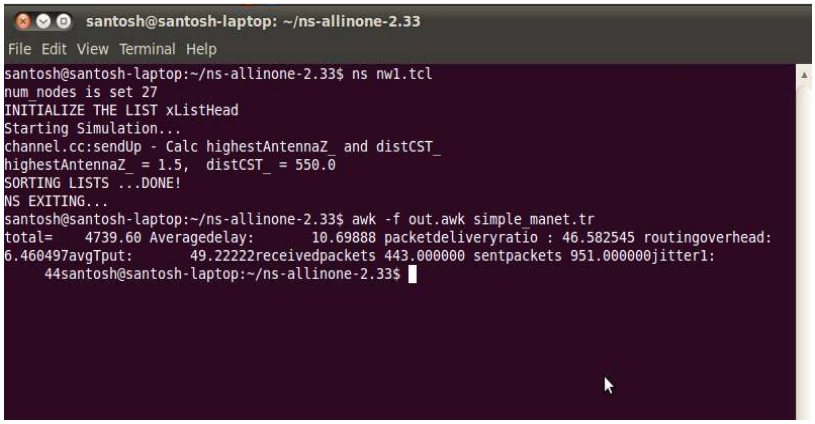

Figure 5: Parameter Results of Scenario 2

Figure 5 shows out of total 951 packets 443 packets are received with drop of 503 packets. The Throughput is 49.22 bps.

Performance Evaluation

The parameters used in our simulation to compare results of network by varying the selfish node are Packets delivery ratio and Average end to end delay.

Packet Delivery Ratio

Is defined as the ratio of the number of packets actually delivered without duplicates to the destinations versus the number of data packets supposed to be received.

Average End to End Delay

Refers to the time taken for a packet to be transmitted across a network from source node to destination node

Table 2: Comparison of Existing and Proposed Scheme

Parameters	One Selfish Node		
	Trusted scheme[13]	DSR[13]	Proposed scheme (Selfish Node)
Packet Delivery Ratio (%)	65	48	63.5
Average End to End Delay (ms)	40	62	13.57

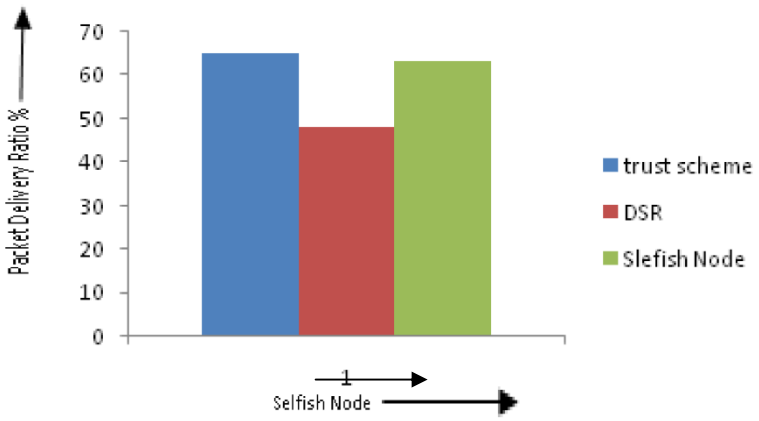

Figure 6: Graph of Packet Delivery Ratio

In Figure 6 green bar shows packet delivery ratio of proposed scheme is 63.5%, in trust scheme PDR is 66% and in normal dsr PDR is 48%. But after using the reputation method with detection of selfish node the packet delivery ratio in proposed scheme is increased by 15.5% compare to normal dsr protocol. Reputation based DSR is able to provide reliable communication. This is because Reputation DSR selects the best route based on the reputation value. But normal DSR collapses when a selfish node is detected.

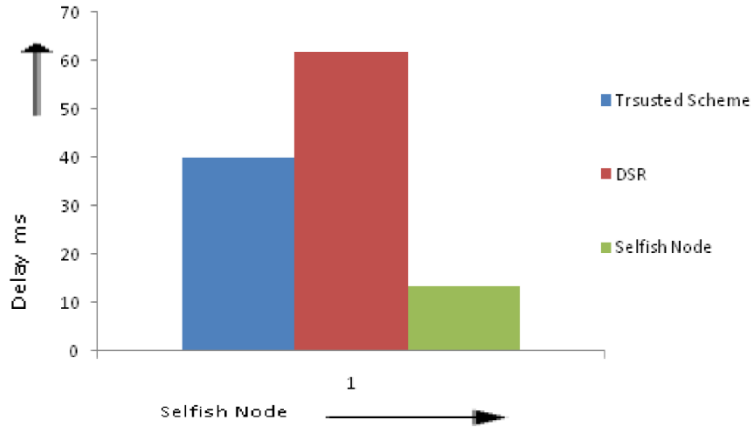

Figure 7: Graph of End to End Delay

In Figure 7 green bar shows delay of proposed scheme i.e. 13.5 ms, in trust scheme Delay is 40 ms and in normal DSR Delay is 62 ms, but after using the reputation method with detection of selfish node the delay in proposed scheme is decreased by 48.43 ms compare to normal dsr protocol. Reputation based DSR is able to provide reliable communication with minimum delay. This is because Reputation DSR selects the best route based on the reputation value. But normal DSR collapses when a selfish node is detected.

We conclude the reputation based Dsr exhibits a better performance in terms of packet delivery ratio and delay with number of mobile nodes as compare to existing solutions.

CONCLUSIONS

DSR is a generally used routing protocol for mobile ad hoc networks but has very low packet delivery rates and poor performance in lightly loaded networks with high node mobility. In this thesis we present how the performance will be improved for the reliable data transmission in MANET by applying the reputation based scheme on the DSR protocol with detection of selfish node. Reputation based DSR is able to provide reliable communication. The reputation DSR selects the best route based on the reputation value. But, normal DSR collapses when number of selfish nodes is increased. The results proved that the detection of selfish node in dsr based Manet using reputation based scheme provides better performance in route discovery in mobile ad hoc network.

REFERENCES

1. Rajesh Sharma & Seema Sabharwal “Dynamic Source Routing Protocol (DSR)”, IJARCSSE, Volume 3, Issue 7, July 2013 pp. 239-241.
2. Sohail Abbas, Madjid Merabti, and David Llewellyn-Jones “A Survey of Reputation Based Schemes for MANET” 2010.

3. Renu Dalal1, Manju Khari and Yudhvir Singh "Different Ways to Achieve Trust in MANET" International Journal on Ad Hoc Networking Systems (IJANS) Vol. 2, No. 2, April 2012.
4. G. Rajkumar, R. Kasiram and D. Parthiban "Optimized QoS Metrics and Performance Comparison of DSR and AODV Routing Protocols", IEEE-International Conference On Advances In Engineering, Science and Management (ICAESM -2012) March 30, 31, 2012. On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012.
5. Santhosh Krishna B.V, Mrs. Vallikannu A.L "Detecting Malicious Nodes for Secure Routing in MANETS Using Reputation Based Mechanism" International Journal of Scientific & Engineering Research, Volume 1, Issue 3, December-2010.
6. Isaac Woungang, Sanjay Kumar Dhurandher, Rajender Dheeraj Peddi and Mohammad S. Obaidat, Fellow of IEEE and "Detecting Black hole Attacks on DSR-based Mobile Ad Hoc Networks", 2012.
7. Ramasamy Mariappan Sangameswaran Mohan "Re-pro Routing Protocol with Trust based Security for Broadcasting in Mobile Ad hoc Network" IEEE 2011.
8. Sangheethaa Sukumaran, Venkatesh. J, Arunkorath "A Survey of Methods to mitigate Selfishness in Mobile Ad hoc Networks" International Journal of Information and Communication Technology Research Volume 1 No. 2, June 2011.
9. Poonam, K. Garg, M. Misra "Trust Based Multi Path DSR Protocol", International Conference on Availability, Reliability and Security IEEE 2010.
10. Sangheetaa Sukumran, Venkatesh Jaganathan, Arun Korath "Reputation based Dynamic Source Routing Protocol for MANET" International Journal of Computer Applications (0975 – 888) Volume 47– No.4, June 2012.
11. Anu Saxena*1, Ved Prakash2, simulation study of AODV and DSR routing protocol in wireless ad-hoc networks IJESR/Aug 2012/ Volume-2/Issue-8/Article No-3/741-748.
12. M. Conti, G. Maselli, G. Turi, and S. Giordano, "Cross-layering in mobile ad hoc network design," *Computer*, vol. 37, no. 2, pp.48–51, 2004.
13. Yaser khamayseh, Ruba Al-Salah, Muneer Bani "Malicious Nodes Detection in MANET" journal of network, vol-7 no. 1, pp.116-125, january 2012.
14. Debdutta Barman Roy, Rituparna Chaki" Detection of Denial of Service Attack Due to Selfish Node in MANET by Mobile Agent" Springer Volume 162, pp 14-23, 2011.
15. Priyanka Goyal, Sahil Batra, Ajit Singh "A Literature Review of Security Attack in Mobile Ad-hoc Networks", International Journal of Computer Applications (0975 – 8887) Volume 9– No.12, November 2010.
16. P.S. Patheja, Akhilesh A. Waoo, Lokesh Malviya "Multipath Dynanic Source Routing Protocol for Ad-Hoc Network", International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, Volume 2, Issue 3, March 2012, pp. 436-439.