ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

A Hybrid Routing Mechanism for Fast and Secure Data Transmission in MANET

Rongali Avataram[1], Dr.B.Prabhakara Rao[2], B.A.S.Roopa Devi[3]

PG Student, Department of Electronics and Communication Engg., JNTU Kakinada University, Andhra Pradesh, India[1]

Senior Prof, Department of Electronics and Communication Engg., JNTU Kakinada University, Andhra Pradesh, India[2]

Research Scholar, Department of Computer Science Engineering, JNTU Kakinada University, Andhra Pradesh, India[3]

Abstract: Due to mobility of nodes, routing protocol selection in MANET is a great challenge because of its frequent topology changes. For fast data transmission, we need a better routing protocol that adapts to topology changes quickly. In this paper, a fast and secure routing protocol which is both proactive and reactive in nature has been implemented. In proactive routing mechanism, each node consists of a routing table, that routing table updates takes place when the topology changes. When a new node is added in the network then the topology of the network will change and it takes some time to converge during that time if we want to send data to destination through that new node immediately, it takes some time to converge and then it will transmit the data. To avoid this problem we are going to use reactive protocol instead of proactive in that time that is until network converge. To avoid waiting time and to transmit data as early as possible, we reduced the packet size and contain only limited fields in proactive protocol structure. By this, the total bit size gets reduced. For security aspect we propose a technique to detecting malicious node by using central agent and back ground processing algorithm. The proposed work is simulated in NS-2 simulator.

Keywords: MANET, Proactive, Reactive, Fast and Secure Protocol, Central agent, Processing algorithm, NS-2.
nclude at least 4 keywords or phrases

I. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) [12] are self configuring networks consisting of mobile nodes that are communicating through multi hop wireless links, without using any centralized access point or existing infrastructure. The nodes change its position often, which mean the mobility [6, 7, and 12] of network. So that nodes have to adopt for the network topology change. So that in ad-hoc networks routing protocol try to minimize the traffic in data transmission. Normal routing protocol in fixed network does not show the same performance in Mobile Ad-hoc Networks. For communication among two nodes, one node has to check that the receiving node is within the transmission range of source (Range of a node is defined with the assumption that mobile hosts uses wireless RF transceivers as their network interface), if yes, then they can communicate directly otherwise, with the help of intermediate nodes communication will take place. Each node will act as a host as well as a router. All the nodes should be cooperative so that exchange of information would be successful. This cooperation process is called as routing. Therefore, all the nodes expected to cooperatively to establish routes instantly. Due to infrastructure less and self organizing nature of ad-hoc networks, it has several applications in the area of commercial sector for rescue operations and disaster relief efforts. MANETs also provides a solution in the field of military battlefield to detect movement of enemies as well as for information exchange among military headquarters and so on [12].

In section 2 we describe the routing approaches in manets. Mainly the manet routing protocols are classified into two types. They are proactive and reactive routing protocols. There is other routing protocol called hybrid protocol which is a combination of both proactive and reactive. In section 3 the proposed technique has been described. In that we discuss the proactive routing mechanism, reactive routing mechanism and security mechanism. Further sections we describe performance metrics [2] and present our simulation work. This work simulated in Network Simulator-2 [5].

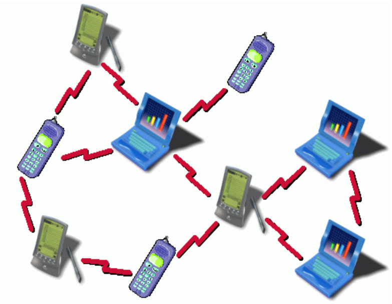

Fig: 1.1 A typical Mobile Ad hoc Network

II. Routing Protocol Classification in MANETS

A Figure 2.1 shows the prominent way of classifying MANETs routing protocols [12]. The protocols may be categorized into two types, Proactive and Reactive. Other category of MANET routing protocols which is a combination of both proactive and reactive is referred as Hybrid.

A. ***Table-driven or Proactive Protocols:*** Proactive routing protocols attempt to maintain consistent, up-to-date routing information between every pair of nodes in the network by propagating, proactively, route updates at fixed intervals.

B. On-demand or Reactive Protocols: Reactive protocols, unlike table-driven ones, establish a route to a destination when there is a demand for it.

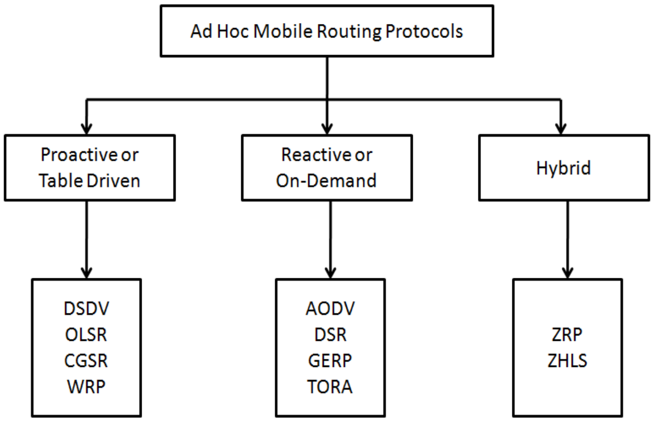

Fig: 2.1 Classification of Ad hoc Routing Protocols

C. Hybrid Routing Protocols: Purely proactive or purely reactive protocols and perform well in a limited region of network setting.

III. Proposed Work

In this proposed protocol, routing is performed through proactive and reactive mechanism. In routers that use dynamic routing protocols, it is important to have fast convergence because routers could make incorrect forwarding decisions until the network has fully converged. In proactive protocol, when a new node is added in the network it takes some time to converge during that time if we want to send data to destination through that new node immediately, it takes some time to converge and then it will transmit the data.

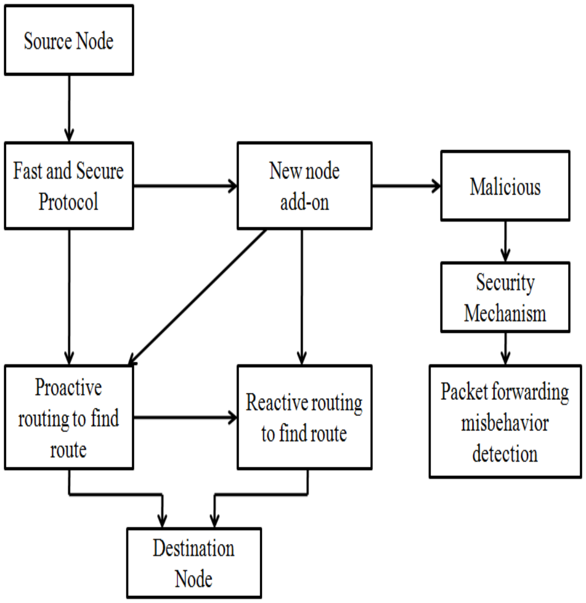
Source Node
Fast and Secure Protocol
New node add-on
Malicious
Security Mechanism
Proactive routing to find route
Reactive routing to find route
Packet forwarding misbehavior detection
Destination Node

Fig: 3.1 Proposed routing protocol Architecture

To avoid this problem we are going to use reactive protocol instead of proactive in that time that is until network converge. Fig 3.1 shows the architecture model of fast and secure transmits protocol [1].

3.1 Proactive routing mechanism to find route

The proposed protocol structure which represented here is similar to Optimized Link State Routing protocol with reduced packet size. Due to its proactive nature, it has an advantage of having the routes immediately available when needed. In this proposed work, the packet structure contains a total of 128 bits. In that packet length contains 16 bits which represents the length of entire packet in bytes. Packet sequence number 16 bits which gets incremented when a new message is transmitted by this host. Message sequence number also inserted into this packet sequence number field itself. Time to live field which maintains the maximum number of hops this message can be forwarded. This field contains only 8 bits. Message type having 8 bits, an integer represents the type of message. In this, message type of 0-127 is reserved for specific protocol and 128-255 is considered for private. Message size field contains 16 bits which maintains the size of the message including header. Originator address field contains 32 bits which specifies the main address of the originator of this message. The proactive routing protocol structure shown in figure 3.1.1

<table>
<tr><td colspan="2">Packet length
(16 bits)</td><td>Packet sequence number
(16 bits)</td></tr>
<tr><td>Time to live
(8bits)</td><td>Message type
(8bits)</td><td>Massage size
(16 bits)</td></tr>
<tr><td colspan="3">Originator address
(32 bits)</td></tr>
<tr><td colspan="3">Message
(32 bits)</td></tr>
</table>

Fig: 3.1.1 Proactive routing protocol structure

3.2 Reactive mechanism to find route

In reactive protocol path discovery is done by sending RREQ and RREP packets. RREQ contains source and destination address, sequence number, broadcast id and hop count. Once the node receives the RREQ, it checks its routing table. If it contains a valid route, it sends RREP to source node. RREP packet contains source and destination address, sequence number hop count and life time of the packet. After finding its path, sender sends the data in next transmission. Then the receiver transmits the acknowledgement in next transmission in normal mode data transfer mechanism [10]. It cause more delay in packet transmission and consumes more bandwidth. In this proposed mechanism, when a node is created and topology is formed, each node will send a message that it can accept the data from the other node. Then any node want to send data will check that message and then send the data along with its route request directly. Receiver sends the acknowledgement for the data in next transmission. By this, we can reduce the round trip time in transmission and we can transmit the data_without any delay.

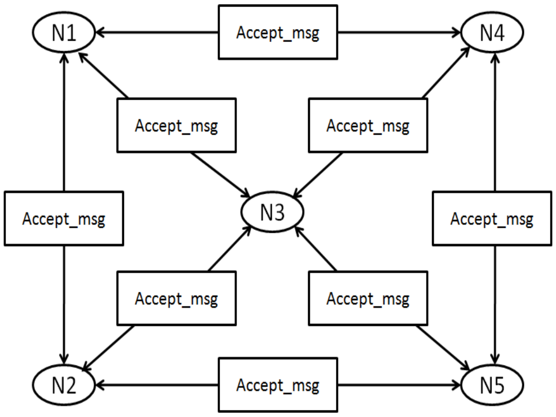

Fig: 3.2.1 Sending Accept_massage to neighbor nodes

In fig.3.2.1, for detecting its route, all the nodes in the topology send accept message to all its neighboring nodes. If any node is already performing transmission with other nodes, it sends busy_ message to its neighbor node and if the node is idle, then it sends idle message to its neighbors as shown in the figure 3.2.2, then it sends the data directly with its route request to the idle node.

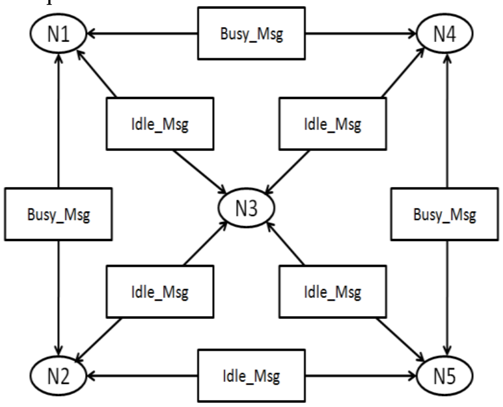

Fig: 3.2.2 Specifications of node modes

When the node detects idle _message from its neighbors, then it can send the data directly along with its route request to the receiver node in a single transmission and the receiver sends the acknowledgement in the next transmission.

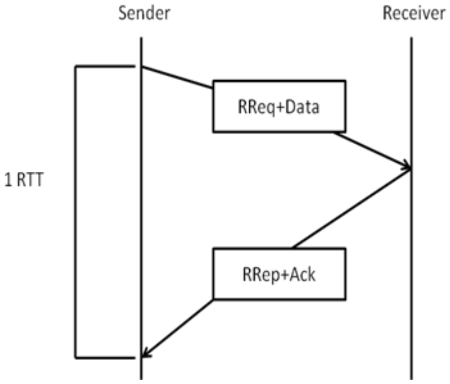

Fig: 3.2.3 First Data Transmission

After finding its path in first transmission, sender sends the packet directly to receiver without sending any route request by its previous route.

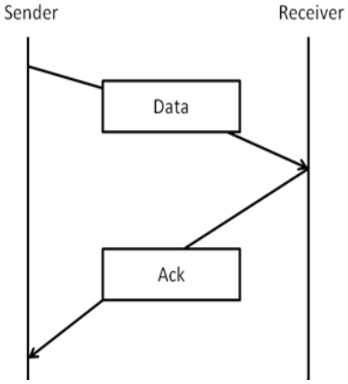

Fig.3.2.4. Direct Data Transmission after first transmission

3.3 Security Mechanism

In MANETs the communication is purely based on trust, without any need of authentication. In this network, each node will communicate with other node using its node information and a malicious node [8, 9] can also join in the network by hacking the node information and acts like a trusted node. This often leads to insecure communication, causing information tampering, DoS, hacking of packets, etc. To avoid this problem we proposed the following technique.

A. Central Agent Monitoring traffic in Network.
B. Background process in each node for monitoring incoming traffic.

A. Central agent monitoring traffic in network

In this mechanism, central agent will maintain the entire node Ids in the network. It also allocates unique id to each node in the network for its identification to monitor the traffic in the network.

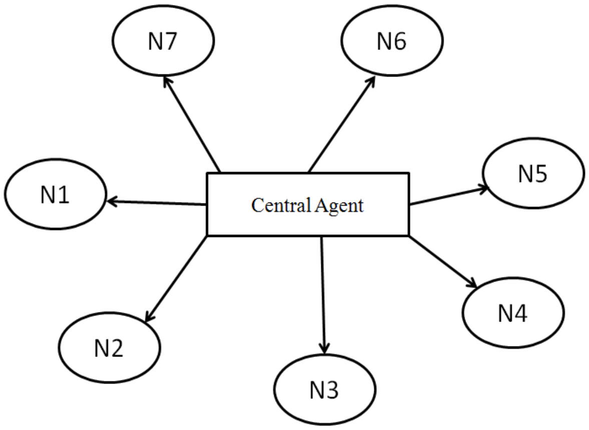

Fig 3.3.1 Central Agent monitoring the traffic in network

This central agent monitors the nodes misbehavior to detect its malicious activity. When a new node is coming with duplicate id or generating more traffic to stop the network services then, it will be detected by that central agent and it will remove it from the network.

B. Nodes with background process algorithm

In this mechanism, processing algorithm is used to detect malicious node by initiating the background process at the each node, this background process will monitor the incoming traffic. The process algorithm is initiated by the central agent and then each node will start the process for monitoring the incoming traffic and it will run in the background of the each node.

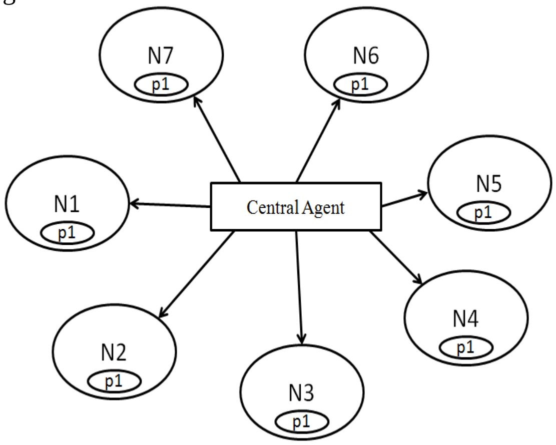

Fig.3.3.2 Nodes with background process

Algorithm for proposed work:

```
Step 1: node Nni creates RREQ = {D, hop_count, seq_no}
Nni sends RREQ to Nc
Nc sends RREQ to Nnexthop
Step 2: If Nnexthop = new node
Check whether it is malicious by processing algorithm
That new node Bj is misbehaving (Detection)
Else
New node Bj is not misbehaving (Non detection)
Endif
Step 3: if new node ≠ malicious
Step 4: then find route using proposed algorithm
Step 5: if Nnexthop ≠ new node
Step 6: then routing perform through proactive
If node ID matches the routing table
Then it will forward the packet
Step 7: if Nnexthop = new node
Then routing perform through reactive
Step 8: send the accept message to neighboring node
If node is busy
Send busy_message
If node is idle
Send idle_message
```

Then send the request and data to the target If target receive the data Then send reply and acknowledgement to sender.

In this algorithm node Nni creates a challenged message and sends the route request to challenged node Nc. Then Nc forward that request to Nnexthop. If the next hop node is a new node, by the detection of packet forwarding misbehavior mechanism, it detects that whether it is malicious or not. This mechanism mainly based on the threshold value of the nodes. If it is not malicious, then routing is performing through a reactive mechanism. It performs routing through proposed fast transmission algorithm. In this, all nodes in the topology first perform communication with its neighboring nodes through accept_message. If any node is already performing with other nodes, it sends busy_message to its neighbor node or nodes and if the node is idle, then it sends idle_message to its neighbors. Then it sends the data directly with its route request to the idle node which performs fast transmission.

IV. SIMULATION DESIGN

In this section we present our simulation results of fast and secure routing protocol by using Network Simulator 2. The simulation time period is 200 seconds, pause time 25sec, interval 0.1sec and the simulated mobility network area is 1000m × 1000m square. To represent ad hoc network we have chosen 50, 60, 70, 80, 90, and 100 mobile nodes.

V. PERFORMANCE METRICS

The following performance metrics are evaluated at different number of nodes.

Packet Delivery Ratio: The ratio of the number of data packets received by the destination node to the number of data packets sent by the source node.

Packet delivery ratio = ∑ Number of packets receive / ∑ number of packet send.

End-to-end Delay: The average time taken by a data packet to arrive in the destination. It includes the delay caused by route discovery latency and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted. End-to-end Delay = ∑ (arrive time-send time) / ∑ number of connections.

Throughput: It is the amount of data that is successfully received at the receiving node by sending node through the network.

Packet Dropped Ratio: It is the ratio of the number of data packets dropped by the destination node to the number of data packets sent by the source node.

Packet dropped ratio = ∑ Number of packets dropped / ∑ number of packet send.

VI. RESULTS AND ANALYSIS

The simulation is done by using network simulator (NS-2) software, with different number of mobile nodes ranging from 50 to 100. Where there is a comparison between with security (green line) and without security (red line).

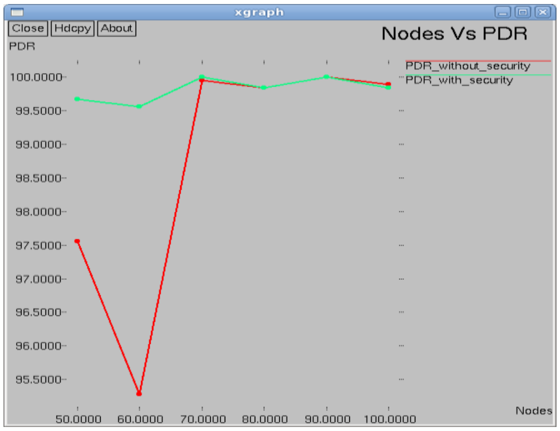

Fig 6.1 Packet Delivery Ration at different number of nodes

In this set of simulation, the number of nodes is varied in the network. The objective of this is to investigate the impact of node density on the protocol performance. The same simulation area is used as in the previous simulations and gradually increases the number of nodes in the network. Figure 6.1 shows the Packet Delivery Ratio (PDR) of the network, that presents minor fluctuations with security, but generally its performance is stable in all cases.

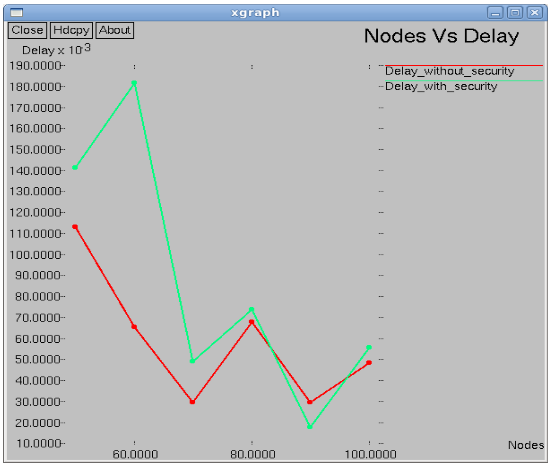

Fig. 6.2 End to end delay at different number of nodes

Figure 6.2 shows the End to end delay of network. Delay at 60 nodes increases exponentially for with security.

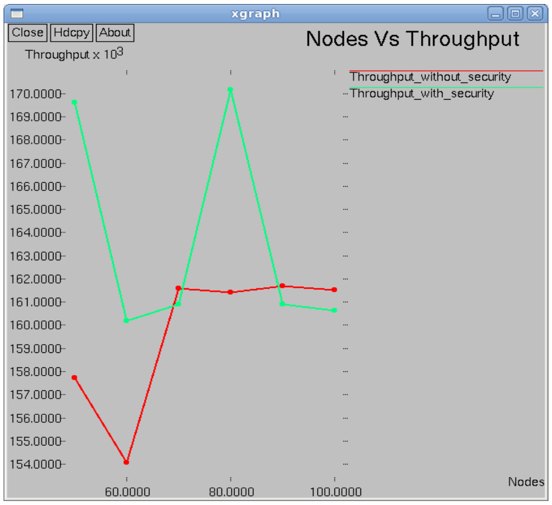

Fig. 6.3 Throughput at different number of nodes

Figure 6.3 shows the Throughput of the network. Its overall performance is good for throughput with security when compared to the without security.

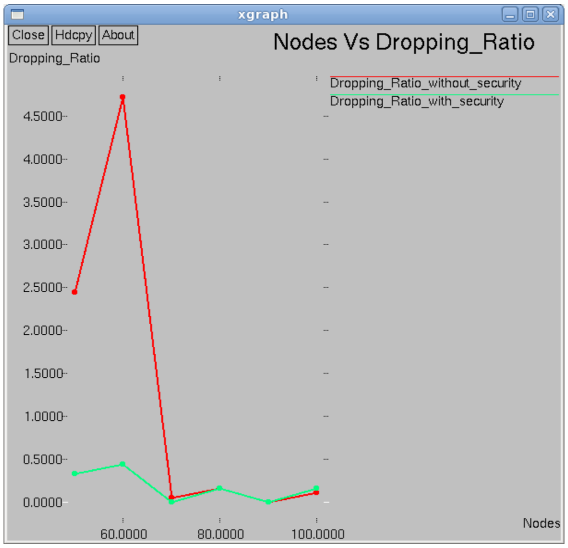

Fig. 6.4 shows the packet dropped ratio of the network.

Figure 6.4 shows the Packet Dropped Ratio (PDR) of the network. It exhibits excellent performance with varying number of nodes for with security.

VII. CONCLUSION

Constantly changing topology of the network makes ad hoc routing protocols incapable of providing satisfactory performance and providing security in MANETs became a great deal. Hence to address this problem, fast and secure routing protocol has been simulated and we have observed the protocol performance by considering different metrics in MANET. In this we are using both proactive and reactive mechanisms for fast data transmission and for providing security a central agent and background process algorithm is further been used and this can be implemented in real time applications.

REFERENCES

[1] B.Thanikaivel and B. Pranisa, "*Fast and Secure Data Transmission in MANET*", International Conference on Computer Communication and Informatics (*ICCCI*-2012), Jan. 10-12, 2012.

[2] Patil V.P, "*Reactive and Proactive Routing Protocol Performance Evaluation for Qualitative and Quantitative Analysis in Mobile Ad hoc Network*", International Journal of Scientific and Research Publications, Volume 2, Issue 9, September 2012

[3] Ajay Vikram Singh, Prof. M. Afshar Alam and Prof. Bani Singh "*Mobility Based Proactive And Reactive Routing Algorithm In Mobile Ad Hoc Networks (Manets)*", International Journal of Computer Science and Information Technologies, Vol. 2 (4), 2011.

[4] Nitiket N Mhala and N K Choudhari, "An *Approach for Determining Conditions for Monitoring of Critical Nodes for MANET Intrusion Detection System* ", International Journal of Future Generation Communication and Networking Vol. 4, No. 1, March 2011.

[5] A Manual of"The *Network Simulator Manual*", by Kevin Fall (Editor) and Kannan Varadhan (Editor). In 4th November 2011.

[6] Sarkar Narul I, Lol Wilford G., "*A study of MANET Routing Protocols: Joint node density, packet length and mobility*", Computers and Communications (ISCC), 2010 IEEE Symposium on, pp. 515-520, 2010.

[7] Yasser Kamal Hassan, Mohamed Hashim Abd El-Aziz, and Ahmed SafwatAbd El-Radi, "*Performance Evaluation Of Mobility Speed Over Manet Routing Protocols* ", International Journal of Network Security, Vol.11, No.3, PP.128, November 2010.

[8] Santhosh Krishna B, Mrs. Vallikannu A.L, "Detecting Malicious Nodes for Secure Routing in MANETs Using Reputation Based Mechanism", International Journal of Scientific and Engineering Research, Volume 1,Issue 3, December-2010.

[9] Manikandan T, Sathyasheela K B, "*Detection of Malicious Nodes in MANETs*", IEEE 2010.

[10] Sabina Barakovic, Suad Kasapovic, and Jasmina Barakovic, "*Comparison of MANET Routing Protocols in Different Traffic and Mobility Models*" Telfor Journal, Volume 2, No. 1, 2010.

[11]] Oscar F. Gonzalez, Michael Howrath, George pavlou "*An Algorothm to Detect Packet Forwarding Misbehavior in Mobile Ad hoc Networks*", IEEE 2007.

[12] A text book of"*Ad hoc and Sensor Networks Theory and Applications*", by Carlos de Morais Cordeiro Dharma Prakash Agrawal. Chapters [1, 2, 10].