ISSN : 2231-0711

Suhasini Sodagudi et al | International Journal of Computer Science Engineering and Technology(IJCSET) | November 2014 | Vol 4, Issue 11,308-313

A Case Based Study to Identify Malicious Node in Packet Routing

Suhasini Sodagudi [#1], Dr.Rajasekhara Rao Kurra [*2]

[#]*Associate Professor, Department of Information Technology,*
VRSiddhartha Engineering College
Vijayawada, A.P. India

[*]*Professor & Director, Sri Prakash College of Engineering, Tuni*
Sri Prakash College of Tech., Rajahmandry
Prakasam Dt,, A.P. India

[1]ssuhasini09@gmail.com
[2]krr_it@yahoo.co.in

***Abstract*— MANET is a standalone ad hoc network with a system of mobile nodes interfacing without any centralized infrastructure. Generally, in the network layer of such an network, there are more possibilities for an attacker to observe traffic and inject themselves into the transmission path between the source and destination. Hence, routing and data forwarding tasks are common issues that are performed in the network. In data forwarding task, forging of identities and falsifying of data are the two common types of attacks that can be launched by an adversary in a multicast routing model. To compensate such data loss, security must be provided. A Systematic approach of routing attacks is in five categories covering impersonation, modification, fabrication, and replay. In this direction, detection of behavioural model of Sybil attack is focused by using network simulator**

***Keywords*— attack, mobile nodes, impersonation, multicast**

I. INTRODUCTION

MANET is a self-configuring network of mobile devices connected by wireless links. Each devices move independently in any direction. Each node acts as a router. Ad hoc networks are temporary that can be setup anywhere without any external infrastructure like wires or base stations. One of the most important issues in designing MANET protocols is to deal with nodes that do not cooperate. It is easy for a node to enter into an ad hoc network which causes mesh confusion. As there is no dedicated authority for routing, packet forwarding, authentication and network management, security becomes an important issue to be addressed.

The main purpose of an ad hoc network routing protocol is to enable the transportation of data packets from one point to another[4]. Depending on their user's motivation the nodes are categorized into three groups as malevolent nodes, selfish nodes, and erroneous nodes. Malevolent nodes are the nodes that want to compromise the security of the MANET or of other nodes. Selfish nodes are the nodes that do not forward other's packets. Erroneous nodes are the nodes with failing hardware or incorrect software.

[2][6]MANET existence consists of closed and open systems. In a closed MANET, all mobile nodes cooperate with each other towards a common goal, such as emergency search/rescue or military and law enforcement operation. [2]In an open MANET, different mobile nodes with different goals share their resources in order to ensure global connectivity. But in some cases some nodes refuses to share its data, called as selfish nodes or misbehaving nodes. Two basic schemes as credit-based and reputation-based are present to avoid the selfish nodes. Credit Based Scheme is for performing network functions and it provides incentive for nodes. Reputation Based Scheme detects and declares the misbehaving nodes in a collective manner and later the nodes are cut off from the network.

ROUTING is selecting a path or route in a network for forwarding packets. The objective of routing packets in a network is to determine the best possible path in terms of minimizing the number of hops, delay, packet loss, cost etc. ROUTING IN MANET is different from traditional routing. In MANET each node acts as both host and router. The nodes transmit and receive their own packets and also take part in forwarding packets for other nodes. Therefore MANET provides limited physical security as compared to the traditional network. [1][7]In general, routing protocols for MANETs are designed based on the assumption that all participating nodes are fully cooperative. One such routing misbehavior is that some selfish nodes will participate in the route discovery and maintenance processes but refuse to forward data packets.

ROUTING Protocol for a MANET can be classified as Proactive and Reactive. Proactive routing protocol is table driven that determine path in advance and periodically exchange routing data to maintain the path. Reactive routing protocol is on-demand that determines a route to some destination node only when it has to send some data. [1][3]The goal of routing in a MANET is to discover the most recent topology of a continuously changing network to find a correct route to a specific node.

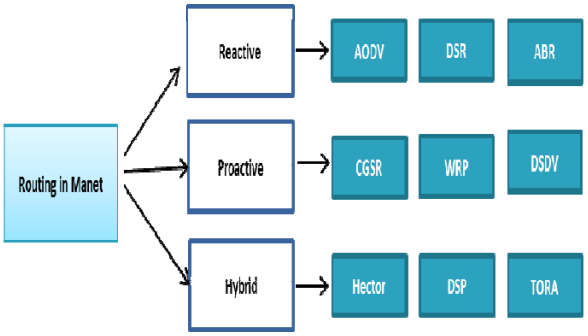

Fig. 1 Routing Protocols Classification

II. RELATED WORK

A. Routing Attacks in Mobile Ad hoc Layering Structure -Routing attacks in Manet can be classified as active and passive attacks. [2][3]In an active attack, attacker attempts to modify or alter the data being exchanged in the network. In Passive attacks attacker snoops the data exchanged in the network without altering it. A Systematic approach of routing attacks is of five categories such as impersonation, modification, fabrication, and replay.

Passive Attacks	• Snooping • Eavesdropping • Traffic analysis • Monitoring
Active attacks	• Wormhole • Black hole/Gray hole • Resource consumption

Figure 2. Network Security Attacks against MANET

Impersonation: In impersonation attacks, an intruder assumes the identity and privileges of another node in order to consume its resources or to disturb normal network operation. Some strong authentication procedures can be used to stop attacks by impersonation. Man in middle attack, Spoofing, Sybil attack comes under impersonation.

Modification: This attack disrupts the routing function by having the attacker illegally modifying the content of the messages. Misrouting attack and Blackmail attack comes under modification.[1][6]

Fabrication: In fabrication attacks, an intruder generates false routing messages, such as routing updates and route error messages, in order to disturb network operation or to consume other node resources. Black hole and grey hole are the examples of routing attacks in fabrication.

Replay attack: In the replay attack, an attacker retransmits data to produce an unauthorized effect. Worm hole and tunnelling attack comes under replay attack.

B. Network Layer Services in Mobile Ad hoc Network

All network activities, such as discovering the topology and delivering data packets, are to be operated by the nodes themselves, either individually or collectively. [5]Depending on this application, the structure of a MANET may vary from a small, static network that is highly power-constrained to a large-scale, mobile, and highly dynamic.

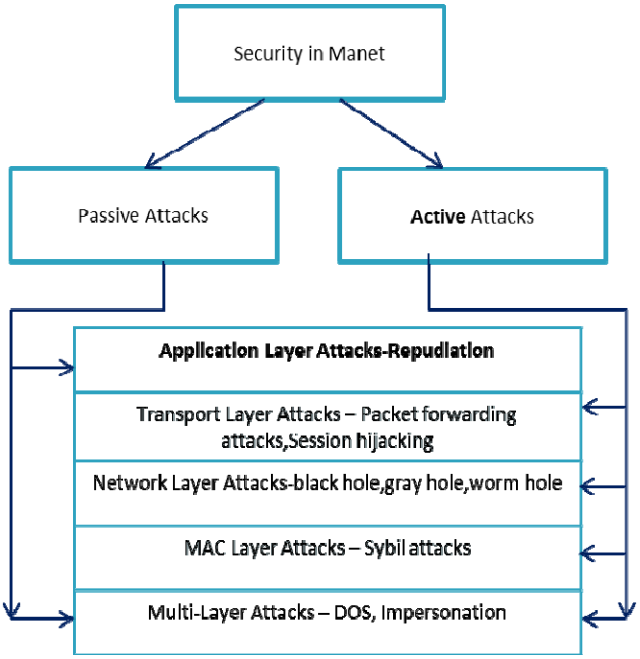

Fig.3 Network Security Attacks against layers in MANET

In routing mechanism of ad hoc networks three layers namely physical, MAC and network layers play a major role. As MANETs are more vulnerable to various attacks, all these three layers suffer from such attacks and cause routing disorders. The variety of attacks in the network layer differs such as not forwarding the packets or adding and modifying some parameters of routing messages; such as sequence number and hop count. [4][5]The most basic attack existing in the network layer is that an adversary node can stop forwarding the data packets. The consequence caused by this is that, whenever the adversary is selected as an intermediate node in the selected route, it denies the communication to take place.

III. LITERATURE SURVEY

In our survey attacks and their countermeasures in mobile ad hoc network for five layers: application, transport, network, data link, and physical. For attacks against the network layer, the survey of countermeasures for identification of misbehaving in manets and selfish node detection. However, in this article, we survey the current state of attacks on the network layer, that is, routing attacks such as Sybil attack in manet. Then, we provide an overview of countermeasures for that attack.

A. Sybil Attack -The Sybil attack in computer security is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks. The Sybil attack can occur in a distributed system that operates without a central authority to verify the identities of each communicating entity. [4]The node spoofing the identities of the nodes is called malicious node or Sybil attacker and the nodes whose identities are spoofed are called Sybil nodes. A Sybil attack is also used by companies to increase the Google PageRank rating of the pages of their customers. Spammers can use Sybil

attack to gain access to multiple accounts on free email systems. Malicious users obtain multiple fake identities. Gain large influence by "Out Vote" honest users. Two routing mechanisms that are vulnerable in Sybil attack in the mobile ad hoc networks is multi path and geographical routing.

B. Procedure to consider a node as misbehaving - In MANETs, routing misbehaviour can severely degrade the performance at the routing layer. In some networks, a router may be considered well-behaved as long as it sends out the packet toward the next-hop node. [9]This, however, does not guarantee the successful reception of the packet at the next-hop node. Such behaviour by the router, if consistently repeated, will be considered as misbehaviour. After all, it is the router's responsibility to make sure of the successful reception of the packet at the next-hop node when it responded to the route-discovery process. One solution to misbehaving node is to forward packets through nodes that share a priori trust relationship. Another solution to misbehaving nodes is to attempt these nodes from within the actual routing protocol for the network

C. Creation of false identities -Node that do not forward other packets thus max their benefits at the expense of all others. They are assumed to always behave rationally. So they cheat only. If a route to a destination is needed it is established at the route discovery phase. It enables dynamic, self-starting multihop routing between participating mobile nodes wishing to establish maintain adhoc networks.

D. AODV Protocol – Implementation
The Currently, several efficient routing protocols have been proposed.. The goal of routing in a MANET is to discover the most recent topology of a continuously changing network to find a correct route to a specific node. In reactive routing protocols, such as the Ad hoc On Demand Distance Vector (AODV) protocol, nodes find routes only when required for a mobile ad hoc network.

In AODV each node has the routing table and each node receives a control packet. [8][9]Three types of message formats are there in Aodv Route Request (RREQ), Route Reply (RREP), and Route Error (RERR).When a source node S wants to send a data packet to a destination node D and does not have a route to D, it initiates route discovery by broadcasting a route request (RREQ) to its neighbors. The immediate neighbors who receive his RREQ rebroadcast the same RREQ to their neighbors. This process is repeated until the RREQ reaches the destination node. AODV allows mobile nodes to respond to link breakages. When link breaks, AODV causes the affected set of nodes to be notified. We have selected AODV because it is one of the leading protocols for manet and uses sequence number to avoid loops. Unicasting and Multicasting is possible.

IV. PROPOSED APPROACH

In the unicast approach is a route from source to destination. It specifies creation of network that defines a simple topology with agents and nodes. Unicast is the term used to describe communication where a piece of information is sent from one point to another point. In this case there is just one sender, and one receiver. Unicast transmission, in which a packet is sent from a single source to a specified destination, is still the predominant form of transmission on LANs and within the Internet. All LAN supports IP networks support the unicast transfer mode, and most users are familiar with the standard unicast applications (e.g. http, smtp, ftp and telnet) which employ the TCP transport protocol.
Normally it involves UDP agent with CBR traffic generator and TCP AGENT for the transmissions of requests. Unicast messaging is used for all network processes in which a private or unique resource is requested. Certain network applications which are mass-distributed are too costly to be conducted with unicast transmission since each network connection consumes computing resources on the sending host and requires its own separate network bandwidth for transmission.

Step 1: Establish a Manet with topology with p-p data collected from Stanford university, 2009

Step 2: Routing structure (seqnum, destination address, and lifetime) establishment from source

Step 3: Broadcasting of a routing table structure from the source node using AODV protocol

Step 4: Verify the attribute seqnum of routing table while in transmission

Step 5: Verify the node behaviour as Anomalous or not

Step 6: Over UDP packets in transmission, validate their sequence

Step 7: Validate Packet transmission is TCP or UDP until destination node along the routing structure

Step 8: If packet = Tcp then transmit the packet

Else drop the packet and designate the transmitted node as selfish node and Anomalous

Fig. 4 Step-by-step process of MRMA

MMRA "mobile misbehaving routing attack" focuses on identification of node behavior an attack can be detected. It just drops the packet or the datagram once it is identified as misbehaving. Generally misbehaves focuses on the desired features such as unintentionally dropping the packets, consuming the network resources, identifying the identities. One of the most fundamental tasks in a mobile ad hoc network is to provide routing capabilities to deliver a data packet from one node to a specific destination node. [7]This point-to-point communication between a given source node and a given destination node is also referred to as unicast.

Overlay network has begun to attract considerable research effort as wireless devices at present. Both network types share a number of key characteristics such as the lack of accentual infrastructure, highly dynamic network topologies, and the need for self-organization. We are using a very simple and straight-forward address resolution scheme. Whenever a node assigns itself a new overlay-id it will publish its new, current overlay-id at a certain location in the network. For this purpose, the node hashes its node address (e.g. its MAC or IP address), next, the node simply routes a packet containing its current overlay-id. The node currently is responsible to store the originator's current overlay-id and thus converts into temporary address server.

A. Step1: Establish a Manet with topology

In particular, when simulation is aimed at testing the scalability of new protocols and applications, working with large-scale realistic network topologies becomes indispensable requirement. In particular, ns2provides researchers with

- Multicast and unicast routing protocols
- Different transport protocols (TCP, UDP, RTP, etc.) The topology generator can generate topology using any standard graph generator (GT-ITM, Tiers etc.). Currently it supports GT-ITM generator only and converts the topology graph into ns format.

B. Step2: Routing structure (seq-num, destination address, and lifetime) establishment from source to destination.

Routing plays an important role in security of the entire network. The knowledge about the topology can dramatically affect the performance of Mobile Ad Hoc Networks[7]. When a node wish to transmit traffic to a host to which it has no route, it will generate a route request (RREQ) message that will be flooded in a limited way to other node CBR is a constant bit rate if one node is travelling or transmitting using CBR it mentions that there always generates traffic on this node.

[6][7]MANET are formed by wireless mobile nodes that communicate without necessarily using the pre-existing network infrastructure such as base station/access point; where each mobile node operates not only as a node but also as a router so that it can send and receive packets as well as forward packets for others.

C. Step 3: Broadcasting of routing table

Initialize the stimulation by specifying Mac/Simple set bandwidth_ 1Mb, set MESSAGE_PORT 42, and set BROADCAST_ADDR. AODV avoids the ``counting to infinity" problem from the classical distance vector algorithm by using sequence numbers for every route. The counting to infinity problem is the situation where nodes update each other in a loop. Each AODV node maintains a monotonically increasing sequence number which is independent of other nodes.

D. Step 4: Verify the sequence number field in routing table

In AODV sequence numbers represent the freshness of the routing information. Nodes increment its sequence number when it generates a new route request or when it generates a route reply. [3]If a node gets multiple route replies for the destination then it will always selects the route to the destination with greatest destination sequence number.

E. Step 5: Verify the node behaviour as Anomalous or non-anonymous

In order to verify node behaviour is an anomaly or not. It is done by if a node gets multiple route replies for the destination then it will always selects the route to the destination with greatest destination sequence number. This ensures that selected route is the recent one. If destination sequence numbers of route replies are same then node will selects the route which has less number of hops to destination.

Routing table management determines whether a route is still active using primary parameters: source sequence numbers, destination sequence numbers, route request expiration timer and route caching timeout. The route request expiration timer is used to invalidate all the entries of those nodes that do not lie on the path from the source to destination. The expiration time depends on the size of network. The route caching timeout is the time beyond which a route is no longer considered to be valid. For each valid route maintained by a node as a routing table entry, the node also maintains a list of precursors that may be forwarding packets on this route. These precursors will receive notification from the node in the event of detection of the loss of the next hop link.

F. Step 6: Over UDP packets in transmission, validate their sequence

Variables which control the number of nodes and how they're grouped are shown by a topology. In the topology the mobile nodes consists of some set of network components such as link layer, interface layer, mac layer, physical layer. Physical layer is used as a wireless channel where a node transmits and receives signals.[8][2] Link layer used to classify the forwarded packets according to their extraction. After setting up the topographic object define a new topographic by loading the flat grid, then configure the AODV protocol by using the mobile nodes in the topology

G. Step 7: Validate Packet transmission is TCP or UDP

Generally subclass Agent or Message Passing is done and then extracts the message id from the message and then append the messages with $message_id. Now attach a new agent by flooding to each node by determining $MESSAGE_PORT.

In the route discovery process the node or each agent maintains a message port with the new agent, flooding, message passing takes place in a sequential manner. If the node doesn't maintain message port in the specified manner or it unintentionally drops the packets then it is considered as a selfish node which is explained in figure [9]An intrusion-detection system (IDS) can be defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity. Intrusion detection is typically one part of an overall protection system that is installed around a system or device—it is not a stand-alone protection measure. In our simulation module we apply IDS module that protect through the selfish node behaviour. A selfish node generally advertises itself as it is having the shortest path to node whose packets it want to intercept.

H. Step 8: In the proposed method, it is observed malicious node exhibiting selfish behaviour from its routing behaviour in capturing UDP packets to actual destination.. AODV maintains the following fields in its routing table for each routing table entry.

- Destination IP Address
- Destination Sequence Number
- Valid Destination Sequence Number flag
- Other state and routing flags (e.g., valid, invalid, repairable, being repaired)
- Hop Count (number of hops needed to reach destination)
- Next Hop
- Network Interface
- List of Precursors
- Lifetime (expiration or deletion time of the route)if any node don't satisfy the characteristics that node tends to be a malicious node.

V. Implementation And Results

NS (VERSION 2) is an open source network simulation tool. It is an object oriented, discrete event driven simulator written in C++ and otcl to separate the control and data path implementations. The simulator supports a class hierarchy in C++ and a similar class hierarchy within the OTcl interpreter. Users creates new simulator objects through the interpreter. The interpreted class hierarchy is automatically established through methods defined in the class TclClass. NS uses two languages because simulator has two different kinds of things it needs to do. On one hand, detailed simulations of protocols require a systems programming language which can efficiently manipulate bytes, packet headers. On the other hand, a large part of network research involves slightly varying parameters or configurations, or quickly exploring number of scenarios. The primary use of NS is to implement network protocols such as TCP, UDP, traffic behavior such as FTP, TELNET, CBR and VBR. Routing algorithms such as DIJKSTRA and many more. It is primarily UNIX based.

NAM (Network Animator) NAM is a tcl/tk based animation tool for viewing Network simulation traces and real world packet traces. It supports topology layout, packet level animation and various data inspection tools. Autonomous systems (from the BGP logs) – a Directed Gnutella P2P network with nodes: 3011 and edges: 5343 were considered for simulation.

```
#Mobile bode configuration after creation of network
$ns node-config -adhocRouting $val(rp) \
            -llType $val(ll) \
            -macType $val(mac) \
            -ifqType $val(ifq) \
            -ifqLen $Val(ifqlen) \
            -antType $val(ant) \
                -propType $val(prop) \
                -phyType $val(netif) \
                -topoInstance $topo \
                -agentTrace ON \
                -routerTrace OFF \
                -macTrace ON \
                -movementTrace OFF \
                -channel $chan_1_
     # extract message ID from message
      if {[lsearch $messages_seen $message_id] == -1} {
          lappend messages_seen $message_id
          $ns trace-annotate "[$node_ node-addr] received {$data} from $source"
          $ns trace-annotate "[$node_ node-addr] sending message $message_id"
     # global ns MESSAGE_PORT BROADCAST_ADDR
     $ns trace-annotate "[$node_ node-addr] sending message $message_id"
     $self sendto $size "$message_id:$data" $BROADCAST_ADDR $port
     10. # create a bunch of nodes
     for {set i 0} {$i < $num_nodes} {incr i} {
        set n($i) [$ns node]
        }
     # attach a new Agent/MessagePassing/Flooding to each node on port $MESSAGE_PORT
     for {set i 0} {$i < $num_nodes} {incr i} {
        set a($i) [new Agent/MessagePassing/Flooding]
        $n($i) attach  $a($i) $MESSAGE_PORT
        $a($i) set messages_seen {}
     }
     # identify events
     $ns at 0.1 "$a(1) send_message 200 1 {first message} $MESSAGE_PORT"
     $ns at 0.119 "$n(3) label \"malicious node\""
     $n(3) color red
     $ns at 0.12 "$ns trace-annotate \"packet drop\""
     $ns at 0.5 "finish"
      # Finish procedure
     .proc finish {} {       }
```

Fig. 5 TCL script to detect malicious node

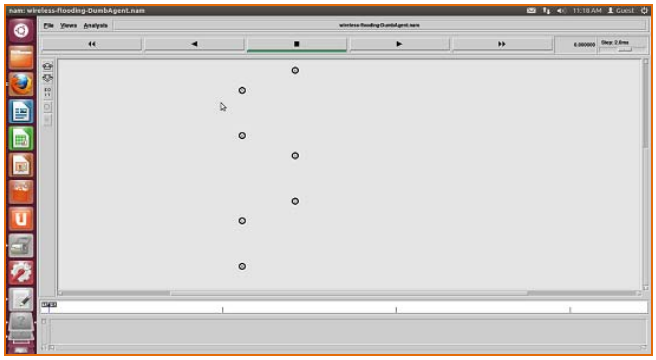

Fig. 6 Mobile nodes simulation in NAM

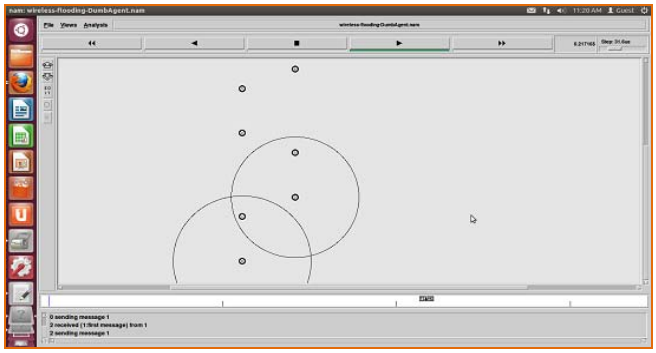

Fig. 7 Mobile Covering Areas as circles

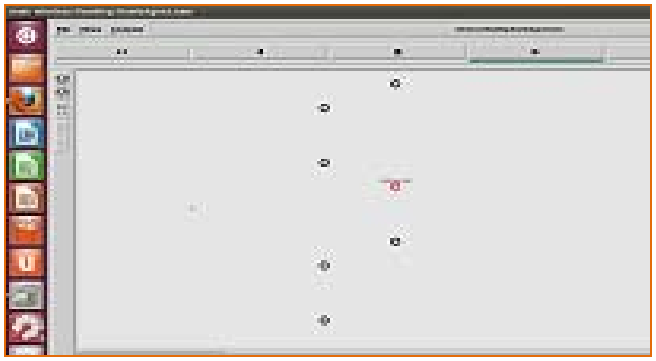

Fig. 8 Red node as malicious from proposed MRMA

VI. CONCLUSIONS

The project aims to develop a solution for identification of behaviour based anomalous nodes within a Manet structure. Usually misbehaviour concept is quite common and dangerous in a mobile network due to its nature as lack of infra-structure. Hence a solution is provided using unicast/multicast routing approach in the network. Routing table is populated using message port that includes the sequence number, host address, destination address. In this work, it is observed with various Manet structures, that a selfish node is almost misbehaving and thereby it is concluded that most of the selfish nodes are anomalous in nature. This anomalous behaviour is studied at the point of packet forwarding. Thus this observed analysis conveys that anomaly is a point anomaly in the network. Future work can be extended to the detection of routing attacks in broadcast approach of a network model.

REFERENCES

[1] K.Liu, J.Deng, P.K. Varshney, and K.Balakrishnan, "An acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETS", IEEE transaction on mobile computing, vol 6.

[2] Suhasini Sodagudi, Dr.K.Rajasekhara Rao, “A behavioral model to identify and analyze anomalous attacks on packet forwarding” IEEE Digital Explore, March 2014

[3] Suhasini Sodagudi, Varun Manchikalapudi, K.Rajasekhara Rao,”An approach to identify anomaly with network data analysis”, IEEE Xplore Digital library, 2012

[4] J Macro Conti, Enrico Gregori, and Gaia Maselli,"Towards Reliable Forwarding for Ad Hoc Networks",IST-2001-38113 MOBILEMAN project.

[5] Suhasini Sodagudi, Dr.K.Rajasekhara Rao, “Behavior based Anomaly detection technique to identify Multilayer attacks”, IJARCSMS, May 2014

[6] L.Zhou and Z.J.Haas. Securing Adhoc Networks .IEEE Network, 13(6):24-30, 1999

[7] Y.Hu and A.Perrig and D.johnson Arriadne: A Secure on demand routing protocol for Adhoc Networks.In proc. Intl Conference on Mobile computing and Networking, sep 2002

[8] Poonam Gupta1, Sarita Chopde2 Detection of routing misbehavior in MANET using improved 2ACK Volume 9, Issue 1 (Jan. - Feb. 2013)

[9] Qinghua Li, Guohong Cao Mitigating Routing Misbehavior in Disruption Tolerant Networks Vol. 7, no. 2, April 2012