Different Trust Based Routing Schemes in MANET

K. Divya*,
*(Ph.D Research Scholar, Department of Computer Science, Gobi Arts & Science College, Gobichettipalayam
mkdivya7676@gmail.com)

Abstract:

MANET is a self configuring network. Due to dynamic nature of MANET it is very challenging work to employ a secure route. The intermediate nodes cooperate with each other as there is no such base station or access point. The routing protocols play important role in transferring data. Cryptographic mechanisms are used in routing protocols to secure data packets while transmitted in the network. But cryptographic techniques incur a high computational cost and can't identify the nodes with malicious intention. Trust mechanism is used as an alternative to cryptographic technique. Trust mechanism secures data forwarding by isolating nodes with malicious intention using trust value on the nodes. In this paper we survey different trust based protocols of MANET and compare their performance.

KEYWORDS -- **Network Protocols, Wireless Network, Mobile Network, Virus, Worms & Trojon.**

- **INTRODUCTION**

This Mobile Ad-Hoc network (MANET) is infrastructure-less, self-configuring network, comprised of several wireless nodes. There are no base stations or routers like wired network for routing the packets. In this network, the nodes behave as a router and discover the routes and maintain the routing of packets. The nodes which are in out-of range of each other can also communicate using some set of rules, called routing protocol and through some intermediate nodes. The main features and characteristics of MANET are

- ***Cooperation:*** In MANET cooperation of nodes is required when a node wants to communicate with a node that is out of its range. In this case, a valid, secure, optimal path is needed for the communication. To find this kind of path cooperation of intermediate nodes plays a vital role.
- ***Dynamic topology:*** The behavior of nodes in the MANET is unpredictable, frequent and random in nature. The nodes can leave or join the network at any time which makes routing very difficult.
- ***Resource Constraints:*** MANETs are comprised of mobile nodes which have limited resources like battery power, bandwidth, low computational capacity etc. So to achieve reliable communication these resource constraints make the task more enduring.

Due to this above discussed nature of MANET, networks are more vulnerable to attacks than wired networks. So security is an important issue in MANET to provide

secure communication between mobile nodes. Sometimes the nodes in the network show misbehavior, depending on which nodes may be identified by two categories: malicious nodes or selfish nodes. Malicious nodes attack the network in several ways to disrupt the normal routing process where as selfish nodes take part in routing but show selfish kind of behavior like selective forwarding, packet dropping etc. Due to all these misbehavior of nodes, performance of MANET degrades. To overcome this problem secure routing protocols need to design which is a more difficult and challenging too. Different approaches are already proposed to secure the routing process in MANET. Cryptographic mechanisms are used in routing protocols to secure the routing information from tampering it by the attacker.

So the trust mechanism is adopted in routing protocols to secure nodes as well as the data transmission. Trust is taken as a parameter while nodes are selected for routing. Trust on nodes may be determined by the direct or indirect communication with the nodes. Different trust based routing protocols are proposed to provide security in MANET by securing nodes in routing path.

- **SECURITY ATTACKS IN MANET**

The routing protocols of the wireless networks should be concerned about the security issues involved in the network more than the wired network for maintaining reliable and secure network as it is easier to launch attacks in a wireless network than wired network. Mobile ad-hoc network is a wireless network and this network has dynamic topology due to the nodes' random behavior. There are four major security issues that is required for maintaining reliable secure network.

- ***Confidentiality***- This means the communication between sender and receiver must be private. The transmitted messages must make sense to only intended receiver.
- ***Integrity***- It means the data arrive at the receiver exactly as they were sent. There must be no change in message during the transmission.
- ***Authentication***- It means the receiver needs to be of sender's identity and that an imposter has not sent the message.
- ***Non-repudiation***- This implies that a sender must not be able to deny sending a message that he or she did send.

A. Wormhole Attack

A worm-hole attack is a serious and severe attack in MANET. In this attack, an attacker captures every control packet in ad-hoc network and tunnels it to another malicious node. This attack disrupts the normal routing by creating the illusion that end-nodes of wormhole tunnel are neighbors but in reality they not. In the fig. two malicious nodes M and N create a false tunnel to forward the packet so that they can tamper the data packets and disrupt the routing procedure.

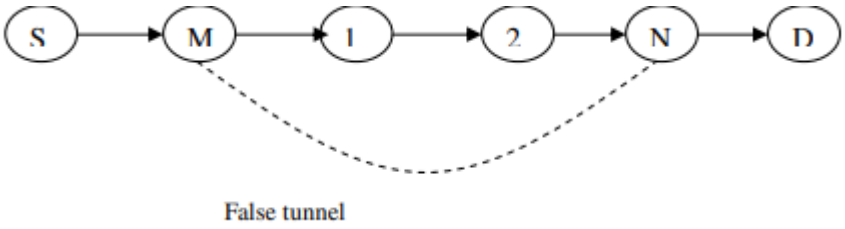

Figure 1 Wormhole Attack

B. Black-Hole Attack

In black hole attack, attacker first involved itself in routing by rushing attack and then capture all the packets coming from the source to a particular destination and drops all the packets destined for that destination. There is a risk for the attacker to be identified as a misbehaving node by the neighbor nodes if there is any monitor mechanism for watching nodes behavior. So sometimes attacker does not drop the packets, but change the information in the packet coming from the source keeping the other information of other nodes intact.

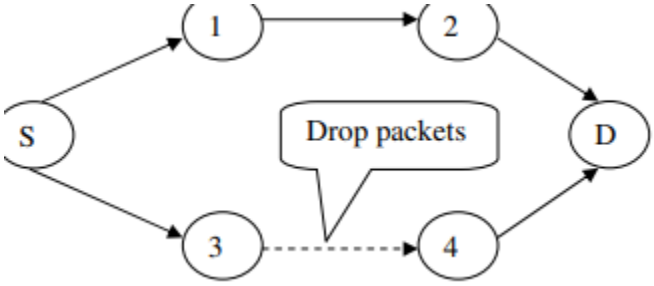

Figure 2 Black-Hole Attack

C. Denial of Service Attack

This type of attack is generally launched by the malicious nodes to flood the network, so that resources of the network like battery power, bandwidth etc are consumed in order to disrupt routing function.

D. Modification Attack

In this attack malicious nodes modify the packet content or insert malicious packets in the network.

E. Sybil Attack

This attack is basically one type of impersonation attack in which malicious node creates multiple fake identities. The node behaves as if there are several nodes instead of one. If there is no identification mechanism of nodes in the network the malicious node generate any arbitrary address to join the network. If there is a mechanism to identify fake nodes the malicious node then tries to steal identity of a valid node. This type of

attack generally occurs in distributed network where no central authority is present to verify nodes identity.

F. Rushing Attack

An attacker captures the route request packet when broadcasted by the source node and immediately forward the packet in the network before the other nodes which also receive the packet. In the following figure, malicious node M forward the request packet first to the destination D and the later request packets from legitimate nodes are discarded. So the destination node D forwards the packets through the malicious node.

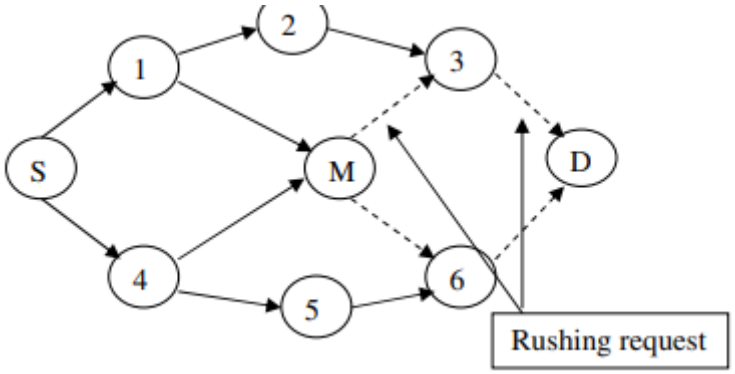

Figure 3 Rushing attack

G. Trust Mechanism

Trust mechanism is introduced in the protocols to provide security in MANET. Trust is a value that is calculated on the basis of nodes action when needed. Trust is introduced to prevent from various attacks like wormhole, black-hole, Dos, selfish attack etc. Trust can be implemented in various ways such as by reputation, subjective logic, from opinion of nodes etc as there are no particular definitions of trust.

- ***Context Dependence*** **-** In some specific context trust relationships are applicable.
- ***Function of uncertainty*****-** Trust depends on the uncertainty of nodes action. It gives the probability of action performed by a node.
- ***Quantitative value*****-**Trust can be assigned any type of numeric values discrete or continuous.
- ***Asymmetric Relationship*****-** Trust relationship is asymmetric in nature. If node A trusts B and node B trust C that does not mean that A trusts C. There are some different representations of trust. Basically, they can be divided into two categories-continuous and discrete numbers. Trust value can be of different ranges.

• ROUTING PROTOCOLS

Routing protocols in MANET are of two types: proactive and reactive protocols. Proactive protocols constantly monitor networks and periodically send messages to all other nodes for up to-date view of network. Every node maintain routing table for all

other nodes and update regularly when any node moves. So these protocols are not suitable for frequently changed wide MANET. Some proactive protocols are DSDV, LSP, R-DSDV, FSR(Fish State Routing), CGSR(Cluster Head gateway switch routing), OLSR(Optimized link state routing), HSR(Hierarchical State Routing), TBRPF(Topology based reverse path forwarding), DREAM(Distance Routing effect algorithm for mobility), STAR(Source Tree adaptive routing protocol) etc. Currently most used reactive protocols are AODV, TAODV, ARAN, DSR, and ARIADNE.

- ***Dynamic Source Routing***

Dynamic Source Routing (DSR) is an Ad Hoc routing protocol which is basically source-based routing. This protocol is source-initiated i.e. data packets carry complete address from source to destination and no routing table is maintained in intermediate nodes. This Protocol mainly has two phases: route discovery and route maintenance. First, source node broadcasts a route REQUEST (RREQ) packet containing a unique ID and the IP address of Destination. When the neighbor nodes of sender receive first copy of the RREQ packet, appends its IP address to the RREQ packet if it has no route to destination and forward RREQ packets again to its neighbors. When a RREQ reaches to the destination or a node which has a route to destination, a route Reply (RREP) packet that contain the IP address of every node forming the route is sent back to source. Multiple copy of RREP packet is returned by the destination node for each copy of RREQ packets it received.

- ***Adhoc On Demand Distance Vector Routing (AODV)***

AODV is a reactive routing protocol designed for ad hoc mobile networks. AODV establishes routes using request and reply messages. When any node has packets to send, at first it searches for the routes to the destination. If the node doesn't have any routes to the destination, it broadcasts route request packet (RREQ) over the network. After receiving RREQ packet, the intermediate nodes update their routing table with the address of the node from which it gets first RREQ broadcast messages and hence it sets a reverse path to that node. The nodes that receive RREQ packets send back RREP packet, if it is a destination node or it has a route to the destination node.
The route will be maintained periodically till the data packets traveled along this path from source to destination. If any node in that path moves from the network link of the path is broken.

- ***Trusted AODV***

In this scheme, AODV protocol is modified implementing node trust and route trust. Two new control packets are added to AODV protocol i.e. trust request packet(TREQ) and trust reply packet(TREP) and routing table is modified by adding one new field: route trust. The RREP packet of AODV is also modified by extending two new fields: neighbor list and route trust.

A. Calculation of Node Trust

All the nodes maintain neighbor table to keep information of frequently changing node and node trust value. Node trust value is evaluated using neighbor's collective opinion. The calculated trust value is stored in neighbor table corresponding to a node.

$$NTV=[NNT(1)+NNT(2)+NNT(3)+\ldots\ldots+NNT(n)]/n$$

B. Calculation of Route Trust

Every node calculates route trust for each route in the routing table at some regular interval. The route trust value is stored in the route trust field of the routing table corresponding to a nodes entry. A new message R_ACK is used to calculate the route trust value. Destination node in each entry in the routing table generates R_ACK packet and send back in reverse path. Route trust value is calculated by the following formulae:

Route trust= (no of packets send by source - no of packets received by destination)

The route with route trust value 0 is the perfect one. If the route trust value is equal to the no of packets sent the route is rejected.

C. Route Discovery

When source node has packets to send it broadcasts RREQ packets. The nodes receive that packet checks their routing table whether the destination node is available or not, if not it rebroadcasts the packet otherwise it sends RREP packet to the source node. After receiving the RREP packets, source node selects three RREP packets that have high route trust value. Then the source node generates the TREQ packets and sends it to all neighbors in the neighbor list of that RREP packet. After receiving the TREQ packet, all neighbors replies with TREP packet to the source node. Then the source node calculates the node trust of the nodes.

D. Cooperation of Nodes

The main idea of CONFIDANT protocol is to identify non-cooperative nodes. A node selects a route based on trust relationships which is built up from experienced routing and packet forwarding behavior of other nodes. Each node monitors the behavior of all neighbor nodes. When any misbehaving node is found, alarm messages are sent to all other nodes in the network.

- ***The Monitor***

This component watches the behavior of nodes during the routing procedure. If any node misbehaves, then the monitor module detects that misbehaving node and immediately calls reputation system.

- ***The Trust Manager***

The trust manager handles ALARM messages. When any misbehaving node is found ALARM messages are sent to all other nodes to inform about that node. The trust manager maintain alarm table and trust table for checking the trustworthiness of alarm.

- ***The Reputation system***

The reputation system maintains the rating of nodes in a table which has 2 field node id and their ratings. The ratings are done according to the type of nodes behavior detected. The rating function assigns greater weights for own experience and smaller for other nodes opinion about that detected node.

- ***Ad Hoc On-Demand Trusted Path Distance Vector (AOTDV)***

Several trust models that have been proposed are of generally two types: centralized and decentralized trust model. In centralized models, there is a central node which maintains trusts of all nodes in the network. In eBay's reputation scheme, trust is calculated in a following way:

Score total = (Sum of positive scores - Sum of negative scores)

In decentralized model, there is no centralized node to maintain trusts of nodes in the network. Several methods are suggested for decentralized trust management. In the paper, trust is computed based on direct interaction among nodes only. Trust is evaluated by packet forwarding ratio (FR). The sender node goes into promiscuous mode and overhears the network to see that whether the neighbor node forwards the packets or not. Let a node j will give trust score to its neighbor k depending on the correct forwarding of packets by node k. Packet forwarding ratio (FR) is the ratio of correctly forwarded packets by a node to the total number of packets sent to that node for forwarding.

- ***Node Trust Computation***

The trust of one node (let j) on another node (let k) depends on the correct forwarding of packets by node k. The direct trust on k by node j (Tjk) at time ti is calculated as the following way:

$$Tjk(ti) = w1*CFRjk(ti)+w2*DFRjk(ti)$$

where CFRjk (ti) and DFRjk (ti) is the control packet forwarded ratio and data packet forwarded ratio of node k observed by node j at time ti respectively.w1,w2 are the weightage given to CFR and DFR. The values in between 0 and 1 implies different trust levels such as the trust value greater than 0.5 means there is a more chance of success than failure and less 0.5 means failure probability.

Table 1 trust Level of Nodes

Level	Trust Value	Meaning
1	[0,0.5]	Malicious
2	[0.5,0.85]	Suspicious
3	[0.85,0.95]	Less trustworthy
4	[0.95,1]	Trustworthy

- ***Path Trust Computation***

When the path from source to destination is discovered the trust of the path is evaluated from the trust of node along the path. The trust of a path P (denoted by Tp (ti) is formulated as:

$$Tp\ (ti) = \min\ (\{Tjk\ (ti) \mid nj, nk \in P \text{ and } nj \rightarrow nk\})$$

Where nj -> nk means nj sends packet to the nk along the path P.

In this paper the following trust record list is proposed to keep track of trust of the next hop nodes. Packet buffer field contains currently sent packets. NC and NA are the two integer counters for control and data packets. Before sending a packet to the neighbor, the sender checks the trust value of the neighbor node and increases NA counter by 1 and if it receives an acknowledgement of correctly forwarded packet NC counter increases by 1.

Table 2 Structure of Trust Record List

Node ID
N_C and N_A for control packets
N_C and N_A for data packets
Packet buffer

- **TRUSTED AOMDV**

AOMDV is a multipath routing protocol. In the paper, a trust mechanism is employed with soft encryption methodology in AOMDV protocol. This Trusted AOMDV protocol has the following steps:

- ***Degree Of Secrecy for Path /Message***

Degree of secrecy of a path implies how much degree of security level required for a path to transfer packets. Degree of secrecy is calculated by the trust value of a node. There are three categorization of security level for path and data packets are used: class A implies top secret, class B implies secret, class C implies confidential. The path trust value (Tp) is the minimum trust value among all nodes along the path p depending upon the path trust value there are three classifications:

- ***Message Encryption***

The message is divided into three parts and then encrypted using soft-encryption methodology to secure the message. It is encrypted in the following way:

a'=aXORc b'=bXORc c'=aXORbXORc

- ***Message Routing***

The trust mechanism of this scheme depends on the monitoring of packets and node's behavior. It is assumed here that when a node sends packets it will monitor its neighbor node to which it sends its packet and determines node's trust value depending on its behavior. If the neighbor node sends the packets correctly node's trust will increase, otherwise it is decreased. The trust value of a node (Tn) is calculated as:

$$Tn = Wd * Td + Wr * Tr$$

where Wd is the weight assigned to direct trust Td, Wr is the weight assigned to recommendation trust Tr . Again Direct trust is calculated as: Td= Td +c. Ts , if no. of successful packet transmission time is high and Td= Td - c .Tf , if the no. of packet

transmission failed time is high. Where Ts is the aggregate successful transfer time, Tf is the aggregate failure transfer time and c is the predefined constant value. Ts is incremented by 1 for every successful transfer of packet, otherwise Tf is incremented by 1.

- ***Trust Based Security Protocol Routing***

In this protocol a trust mechanism is employed in DSR protocol. An extra data structure is maintained by every node that is Neighbor's Trust Counter Table (NTT) which is used to keep track of no. of sent packets by a node using a forward counter (FC) and also stores the trust counter(TC) corresponding to node. Initially a node can completely trust its neighbor or fully distrust its neighbor as the nodes don't have any information about its neighbor nodes reliability. When any node needs to send data it broadcasts RREQ packets. Each time a node (let nk) receives packet from another node (let ni), node nk increments the FC of ni as:

$$FCni=FCni+1;\ i=1, 2\ldots.$$

Then this new FCni value is stored in NTT of node nk. After receiving all RREQ packets, destination node makes a MAC on the no of packets it received (Prec) using the shared key between the sender and destination. Then the destination node attaches that MAC and also the accumulated path from the RREQ after digitally signed it, in the RREP packet and sends back in the reverse path to the destination. The intermediate nodes of that path determines Success ratio as: -

$$SCni=FCni\ /Prec,$$

where Prec is the no of packets received at destination. This SCni is appended in RREP packet. Another comparison is made by comparing trust counter with a minimum threshold. If trust counter is less than the trust threshold value the node is marked as malicious. This mechanism is applied to all the other routes and a route with no or least malicious node is selected. In this way, a trusted and authenticated route is found for secure routing.

- ***Trust Based DSR***

This protocol is proposed to improve the security of the existing DSR protocol. The trust based secure route is established in this scheme. In DSR the shortest route is selected which may not be secure. There are some malicious nodes in the network that replies to the route request packet with shorter hop count (black hole) so that the source will select that path, and routing process is disrupted. The following components are used in this newly proposed protocol: Initialiser, Upgrader, Administrator, Monitor, and Router. In this scheme, there is a separate administrator to maintain the trust values of all other nodes. An acknowledgement module is there which is used to keep track of all received acknowledgements and trust values of nodes are adjusted. Every node has trust value which depends on its interaction with its neighbor. Trust unit of this scheme comprises of three modules: - Initialiser module assigns low trust values to the unknown nodes in initial stage. If the route contains some known and unknown nodes, then it assigns trust of those known nodes as the initial trust value of the unknown nodes. Upgrader module upgrades the trust value of a node based on experiences of that node in

a particular situation. If any reply is not received by a node the trust value of the neighbor node is decreased. Trust value is evaluated as:

T= tanh[(+W) *Te]

where T is the updated trust, Te is existing trust, W is a weight i.e. 1 for acknowledgements and 0.5 for data packets forwarded and received, is +1 for positive and 0 for negative experiences.

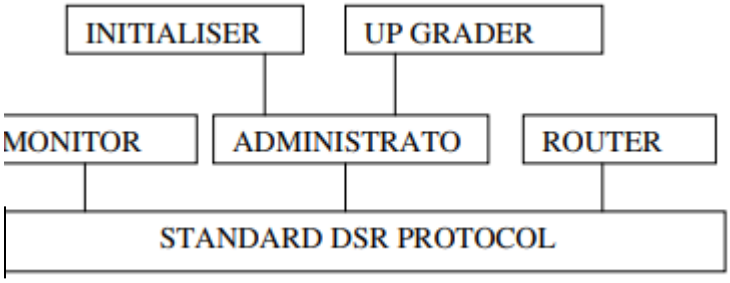

Figure 4 Components of TDSR

- **TRUST MANAGEMENT FRAMEWORK FOR DETECTING MALICIOUS PACKET DROPPING NODES IN A MOBILE AD HOC NETWORK**

In this proposed scheme, it is assumed that each node monitors its neighbor node to know whether it forwards the packet to the next node or not. If any suspicious behavior of a node is detected the trust mechanism is used to determine whether the suspected node is malicious or not. Every node runs some security modules.

- ***Monitor Module***

This module of every node monitors the behavior of its neighbor node to see whether it behaves properly or not. If any abnormal behavior of a node like packet dropping, tampering with packet content.

- ***Reputation Collector Module***

When this module is invoked the accuser node challenges the accused node to verify its behavior. After receiving this challenge from the accuser node, the accused node broadcasts verify _behavior message to its entire neighbor. After getting the verify behavior message, all the neighbors of the accused node send back reply to the accused node with the observed value of degree of maliciousness of its.

- ***Reputation Formatter Module***

This module helps in exchanging reputation of a malicious node over the network. An accused node sends rep_request message to its entire neighbor when it needs reputation value of itself .The neighbor nodes send back reply by sending rep_reply message to the accused node with reputation value of that node.

- ***Reputation Maintainer Module***

A global trust state for all malicious nodes is maintained in a reputation table which has two fieldnode_id and rep_val. The job of this module is to verify the group trust value received from the accused node and update the trust state of that node. The trust value of a node is calculated by the following formulae:

$$(1\text{-Tnew}) = \alpha\,(1\text{- Told}) + \beta.(1\text{-Tcertificate}) - \delta$$

where Told,Tnew and Tcertificate represents old trust, new trust and group trust value respectively. β, α are the weightage of old and new trust value and δ is the trust replenishment factor over time.

- ***Reputation Propagator Module***

This module propagates the trust certificate using the nodes mobility. When new trust certificate of a node is issued it distributed to all the neighbor nodes that are in 1-hop distance from the accused node. The neighboring nodes dynamically exchange trust certificate at a regular interval. The trust certificates are exchanged with the routing packets so no extra overhead. Every node get certificate through flooding and exchange when the accused node moves in the network.

- **CONCLUSION AND FUTURE WORK**

MANETs are vulnerable to different types of attacks due to its infra-structure less network. Different trust based approaches are proposed to prevent such types of attacks and to improve Quality of Services (QoS). These trust based approaches try to give a secure node in routing path by implementing trust mechanism in the existing routing protocols. In this paper, firstly we have given a brief idea on several types of attacks that MANET suffers and trust mechanism. The attacks like wormhole, impersonation, Sybil attack etc still exists in some of the protocol such as trusted AODV, CONFIDANT. As in CONFIDANT protocol the reputation of a node is increased when it forwards he packet so the malicious node that create wormhole get high reputation value.

Most of the protocols like TDSR, SRT etc consider some performance matrices like packet deliver ratio(no of successful packets/no of packets forwarded), average end to end delay to forward packets to the destination and get back reply, communication overhead, route selection time, throughput etc. to measure the performance.
After going through this comparison, we have seen that there are still many scope of work towards the development of a new trust mechanism by considering QoS as well as minimizing the several attacks. A newly developed trust mechanism we can apply in various environments like in hybrid environments. We can also develop some rules in the protocol on the basis of which the actions are taken to detect the nodes that are authenticated but perform malicious behavior without dropping packets and also authenticate the nodes to prevent attacks.

- **REFERENCES**

- Essia T, Razak A,Khokhar R S, Samian N, *Trust-Based Routing Mechanism in MANET*, Design and Implementation. Springer, 18 June 2011.
- Huang J, Woungang I, Chao H, Obidant M, Chi T, Dhurandher S K, *Multi*-Path Trust –Based Secure AOMDV Routing in Ad Hoc Networks. IEEE 2011.
- A M Pushpa, *Trust based secure routing in AODV routing protocol*, International Conference on Internet Multimedia Services Architecture and *Applications* (IMSAA), USA, IEEE, (2009).
- Supriya & M Khari, *MANET Security Breaches Threat to a Secure Communication Platform*, International Journal on Ad hoc Networking System (IJANS), Vol. 2, No. 2, (2012).
- C. Perkins, E. Belding-Royer, S Das, *Ad hoc on demand distance vector (AODV) routing*, RFC 3561.
- Sen, *A Distributed Trust Management Framework For Detecting Malicious Packet drop-ping Nodes In a Mobile Ad Hoc Network*, International Journal of Network security & Its applications(IJNSA), Vol. 2, No. 4, October 2010.
- Nagrath P, Kumar A, Bhardwaj S, *Authenticated Routing Protocol Based On Reputation System For Ad-Hoc Network*, International Journal on Computer Science and Engineering Vol. 02, No. 09, 2010, 3095-3099.
- N Garg & R P Mahapatra, *MANET Security Issues*, IJCSNS International Journal of Computer Science and Network Security, (2009).
- M Dasgupta, S Choudhury & N Chaki, *Routing Misbehavior in Ad Hoc Network*, International Journal of Computer Applications (0975 -8887).
- D B Johnson, D A Maltz & Y C Hu, *The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)*, IETF Draft, (2003).