A COMPARATIVE STUDY ON DIFFERENT TRUST BASED ROUTING SCHEMES IN MANET

Mousumi Sardar[1] and Koushik Majumder[2]

Department of Computer Science & Engineering,
West Bengal University of Technology,
Kolkata, India

ABSTRACT

A mobile ad hoc network is a wireless network in which no infrastructure is available. 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. So, employing cryptographic techniques in MANET are quite impractical as MANETs have limited resource and vulnerable to several security attacks. 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 performances.

.

KEYWORDS

Network Protocols, Wireless Network, Mobile Network, Virus, Worms &Trojon

1. 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. Each node has wireless transmitter and receiver with it, so that it can communicate with each other in a wireless environment. 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 [1] are:

1. *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. Without cooperation of nodes it would be never possible to communicate with out of range nodes.
2. *Dynamic topology*: The behaviour 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. Due to this randomness of nodes, the topology of the network can change at any time which creates a big challenge in MANET design.

3. *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 misbehaviour, 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 behaviour like selective forwarding, packet dropping etc. Due to all these misbehaviour 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. But this approach can't be deployed in real MANET network because of high computational cost and it can't identify the attacker nodes. This mechanism only secures the routing information from tampering but can't secure nodes that participate in routing. 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.

2. 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. For this reason, maintaining security in MANET becomes a challenge for the designers and researchers. 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.

Security attacks are mainly of two types: Active and Passive. In passive attack, an attacker just listens and captures important information rather than modifying it. But in active attack, attacker modifies the data. An active attack is initiated by malicious node to disrupt routing function in a MANET. Some examples of this type of attacks are [2-4]:

2.1. 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. This attack is difficult to detect. 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.

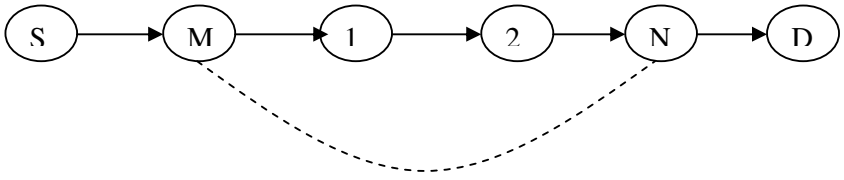

Figure1. Worm-hole attack

2.2. 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.

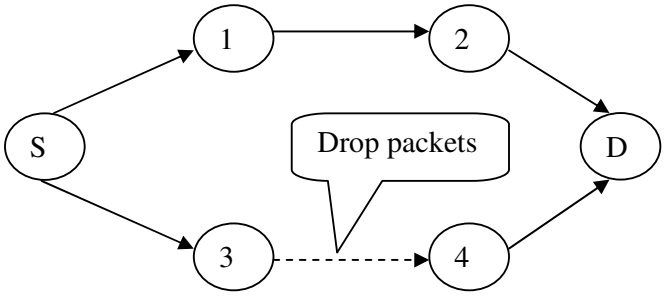

Figure 2**.** Black-hole attack

2.3. 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.

2.4. Modification Attack

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

2.5. 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. Due to this attack the normal routing process is interrupted by the malicious nodes. These malicious nodes create the

illusion of fake routes and when any node sends data through these routes, the packets are dropped or tampered.

2.6. 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. When the packets from other nodes arrive the receiving nodes treat the packets as duplicate packets and discard the packets. 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.

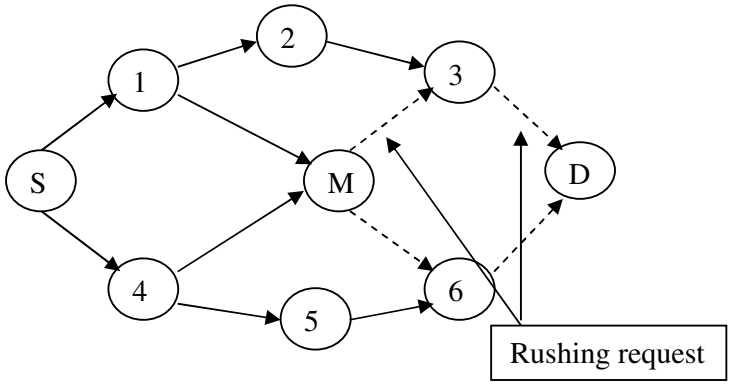

Figure 3. Rushing attack

3. 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. According to (Marc Branchaud, Scott Flinn) trust has following properties:

- *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. For example, trust value can be continuous number 0,1,2,3 where different trust levels are assigned to that continuous values i.e. 0 means no trust, 1 means suspected and so on.

4. EXISTING 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. Reactive protocols [5] rely on some request-reply messages. It is on-demand protocol i.e. when source requests for connection to destination then these protocols establish routes to destination. Currently most used reactive protocols are AODV, TAODV, ARAN, DSR, and ARIADNE.

4.1. Dynamic Source Routing (DSR) [6, 7]

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. As a result source is able to know more than one path to destination. In Route maintenance, the route is constantly monitored and if any failure occurs in the path, the nodes are informed about that failure.

4.2. Ad Hoc on Demand Distance Vector (AODV) Routing [8, 9]

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. After receiving the RREP packets, source node starts to forward the data packets through that path which has minimum hop count. The route will be maintained periodically till the data packets travelled along this path from source to destination. If any node in that path moves from the network link of the path is broken. When any node of that path detects the link failure immediately informs the source node by sending route error message so that the sender node stops sending the data packets.

4.3. Trusted AODV [10]

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: neighbour list and route trust.

4.3.1. Calculation of Node Trust

All the nodes maintain neighbour table to keep information of frequently changing node and node trust value. Node trust value is evaluated using neighbour's collective opinion. The calculated trust value is stored in neighbour table corresponding to a node. Node trust is calculated by observing the behaviour of each node. The node trust value (NTV) of a node i is calculated by the following formulae:

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

where NNT is the neighbour node trust value about the i node and n is the no of neighbour in the neighbour list.

4.3.2. 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. The nodes that receive R_ACK calculate the route trust value using the value in the no_of_packets_received field of R_ACK packet and the value of no_of_packets_sent field in the routing table. 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.

4.3.3. 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 neighbours in the neighbour list of that RREP packet. After receiving the TREQ packet, all neighbours replies with TREP packet to the source node. Then the source node calculates the node trust of the nodes. Next, the source node arrange the RREP packets in the ascending order based on node trust value and selects the first RREP packet and hence that path is selected for communication.

4.4. Cooperation of Nodes: Fairness in Dynamic Ad-hoc Networks [11]

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. As a result, all nodes in the network will be able to avoid that misbehaving node while selecting a route. The components of CONFIDANT protocol works as follows:-

4.4.1. 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.

4.4.2. 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.

4.4.3. 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. The rating of a node is updated when sufficient proof of the nodes maliciousness is found. If the rating falls below threshold value path manager module is called.

4.4.4. The Path Manager

The path manager manages the routing path according to ratings of the nodes. The path containing malicious nodes are deleted by this module. If any route request comes from malicious node path manager takes appropriate action like ignore request or don't reply etc.

4.5. Ad Hoc On-Demand Trusted Path Distance Vector (AOTDV) [12]

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:

$$\text{Scoretotal} = (\text{Sum of positive scores} - \text{Sum of negative scores})$$

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 Pirzada and McDonald [12] proposed aggregation mechanism, where nodes calculate trust according to multiple observed events including acknowledgements, packet precision, route replies, and blacklists.
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 neighbour node forwards the packets or not. Let a node j will give trust score to its neighbour 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. Let N_C (t) is the no of correct forwarding, N_A (t) is the total no. of packets sent to a node for forwarding before time t. Therefore, FR= N_C (t)/N_A (t). If any node doesn't forwards the packets FR value of that node will decrease. Depending on the packets type generally used in MANE, FR is divided in two types: control packet forwarding ratio (CFR), data packet forwarding ratio (DFR).

4.5.1. 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 (T_{jk}) at time t_i is calculated as the following way:

$$T_{jk}(t_i)=w_1*CFR_{jk}(t_i)+w_2*DFR_{jk}(t_i)$$

where CFR_{jk} (t_i) and DFR_{jk} (t_i) is the control packet forwarded ratio and data packet forwarded ratio of node k observed by node j at time t_i respectively.w1,w2 are the weightage given to CFR and DFR. The following table represented the various level of trust on a node depending trust

value. The trust value is ranging from 0 to 1.0 means no trust and 1 means complete trust. 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

4.5.2. 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 $T_p(t_i)$ is formulated as:

$$T_p(t_i) = \min(\{T_{jk}(t_i) \mid n_j, n_k \in P \text{ and } n_j \rightarrow n_k\})$$

Where $n_j \rightarrow n_k$ means n_j sends packet to the n_k 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. N_C and N_A are the two integer counters for control and data packets. Before sending a packet to the neighbour, the sender checks the trust value of the neighbour node and increases N_A counter by 1 and if it receives an acknowledgement of correctly forwarded packet N_C 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

4.5.3. Route Strategy

The route strategy of this algorithm works as follows: When a node has data to send it searches for the destination in its routing table. If the destination node is in table or a node having route to the destination, it selects that route and sends data to the destination. If it is not sender initiates route discovery. The sender first broadcasts RREQ packets which have two additional fields: required trust (RT), actual trust (AT). RT is the required trust for the data packets means RT depends on the importance of data packets and it is set by the sender. AT is the minimum trust value among all the trust value of nodes that RREQ travels during route discovery. When any intermediate node (let j) receives the RREQ packet from a node (let k), node j first checks whether the packet has already received or not. If so the packet is discarded otherwise set a reverse route to source through node k and the path trust is set to minimum of AT and T_{jk}. If node j has a route to destination, it sends back RREP to the source node otherwise it rebroadcasts the RREP packet after modifying path trust value to min (AT, T_{jk}). After getting all RREP packets,

the route with least hop count with required path trust value is selected. If a suitable route is not found, it tries again with a maximum threshold value. If the route is found sender sends data to the next hop and overhear to ensure that whether the packet has forwarded or not. If any node doesn't forward the packet sender just go for the alternative path. If the packet is correctly forwarded sender node update its trust table.

4.6. Friendship Based AODV (FrAODV) [13]

In this paper, friendship based protocol is proposed based on AODV. There are two evaluation algorithms to evaluate forward and reverse path between source and destination. In this scheme, it is assumed that each node has identity can't be forged by any other malicious node and no of malicious node is less than the no of good nodes. In this proposed scheme every node has a list of friends with friendship values. The range of friendship values is 0 to 100. More the friendship values means more trustable. The two algorithms for establishing path are described as follows:

4.6.1. RvEvaluate Algorithm

This algorithm sets up reverse path from destination to source. When a node has packets to send it broadcasts RREQ packet in the network. After broadcasting RREQ packet the two things can happen: -

Case-1: The receiving node can be destination node itself. If so it checks the friendship value of the node from which it receives the RREQ packet, as every node maintains a friendship list along with friendship value of the neighbor nodes. If the node is not a friend the node rejects the RREQ packet. Otherwise it calculates the friendship value of the route to originator from destination and then compares the current routes friendship value with the existing route's friendship values. The reverse route's friendship value (RvFwRte) is the sum of friendship values of all nodes in that path and it is calculated as follows:

$$\text{RvFrRte} = \sum_{i=1}^{n} \frac{\text{PrFrHpi}}{h}$$

Where $PrFrHp_i$ is friendship value of that node from which the current node receives RREQ packet and h is the no. of hops between source and destination. . If the friendship value of the new route is less than the existing route the new route is rejected otherwise it is registered as a friendly route.

Case-2: If the receiving node is intermediate one, it first checks the friendship value of the node from which it receives the RREQ packet and next neighbor node. If one of these two nodes is not in friend list, the intermediate node rejects the RREQ packet. Otherwise it calculates the friendship value of the route to originator from destination using the previously mentioned formulae and compares it with the existing route's friendship value. If the friendship value of the new route is less than the existing route the new route is rejected otherwise the reverse path is established from current node to the previous node.

4.6.2. FwEvaluate Algorithm

This algorithm sets up the forward path i.e. from source to destination. After receiving RREQ packet from sender the destination node creates RREP packet and sends back to the previous hop. There are following two cases when any node receives that packet:

Case-1: If the node receiving the RREP packet is sender node itself, it checks the friendship list and the friendship value of the node from which it receives the RREP

packet i.e. the next node. If the next node is not a friend, rejects the RREQ packet. Otherwise it calculates the friendship value of forward route to destination and then compares it with the existing route's friendship value. If the friendship value of the new route is less than the existing route the new route is rejected otherwise it is registered as a friendly forward route. If there is not any existing route the new route is included as a friendly route. The forward path's friendship value is formulated as:

$$FwFrRte = \sum_{i=1}^{n} \frac{FwFrHpi}{h}$$

Where $FwFrHp_i$ is friendship value of that node from which the current node receives RREP packet and h is the no hops between source and destination.

Case-2: If the node is an intermediate node then it checks the friendship value of the node from which it receives the RREP packet and previous node. If one of these nodes is not friend, rejects the RREP packet. Otherwise it calculates the friendship value of the route to destination in the same way and compares it with the existing forward route's friendship value. If the friendship value of the new route is less than the existing route the new route is rejected otherwise the forward path is established from current node to the next node.

In this protocol the authentication of every node is done using IP and MAC address. In this way after establishing friendly path from source to destination the sender sends data packet along that path.

4.7. Secure Routing Using Trust (SRT) [14]

In this paper, a secure routing using trust level is proposed. This scheme is based on node transition probability (NTP) and AODV. This scheme develops a new algorithm to secure NTP protocol. A trust rate (Trate) is calculated as a parameter. When a node has data packet to send, it first floods control frame (beacon) in search of secure and reliable route. After broadcasting the first beacon trust rate is evaluated as:

$$Trate=\frac{(r-t)}{r}$$

Where r = no of beacons received by a node, t = no of beacons send by a node. This Trate value divides the nodes of the network into 3 categories: ally list, associate list, acquaintance list. Where ally list implies level2, associate list implies level1 and acquaintance list implies level 0.

Ally list: The nodes of the ally list send highly secured information.
Associate list: The nodes of this list send medium secured information.
Acquaintance list: The nodes of this list send the information that do not require any security.

An additional field "level" is there in neighbor table. When a node has data to send it just checks its neighbor table, if the destination is available it just sends data packets. If not, it searches for a node which has route to destination in its same level. If no suitable node is not found it goes to next lower level and so on. If any node in the same level is not found trust is compromised by choosing a neighbor in the next lower level using the following formulae:

Trust compromise= n (associate) + 2*n (acquaintance)

Where n (associate) is the no of nodes in associate list and n (acquaintance) is the no of nodes in acquaintance list. When all the nodes including destination node are in the same level with the source node trust compromise will be very low because trust rate is very high as it is better to forward control packets in the same level than to forward the packets to the another level. In this way after finding secure route the data packets are sent to the destination.

4.8. Trusted AOMDV [15]

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:

4.8.1. 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 (T_p) is the minimum trust value among all nodes along the path p depending upon the path trust value there are three classifications: - If $T_p \geq 8$ implies class A paths. All the class A paths have degree of secrecy≥8. $T_p \geq 5$ implies class B paths. All the class B paths have degree of secrecy≥ 5. $T_p \geq 3$ implies class C paths. All the class C paths have degree of secrecy≥ 3. This classification is also applied for data packets. Class A data only is transferred to class A category path. It is same for other categories.

4.8.2. 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

4.8.3. Message Routing

Before routing the encrypted messages a secure trusted path is established using the following trust mechanisms:-

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 (T_n) is calculated as: $T_n = W_d * T_d + W_r * T_r$ where W_d is the weight assigned to direct trust T_d, W_r is the weight assigned to recommendation trust T_r. Again Direct trust is calculated as: $T_d = T_d + c. T_s$, if no. of successful packet transmission time is high and $T_d = T_d - c .T_f$, if the no. of packet transmission failed time is high. Where T_s is the aggregate successful transfer time, T_f is the aggregate failure transfer time and c is the predefined constant value. T_s is incremented by 1 for every successful transfer of packet, otherwise T_f is incremented by 1. The trust table values determined through hello message transmission. When a node receives hello message it first check trust table contained in hello packet and find some common nodes it has. If any node common node is found that wants to participate in forwarding packets the trust recommendation (T_r) is calculated by the formulae:-

$$T_r = \sum_{X=0}^{n} 0.1 * Td(A \rightarrow X) * Td\ (X \rightarrow D)/n$$

Where $Td(A \rightarrow X)$ implies source A's trust on intermediate node X and $Td(X \rightarrow D)$ implies X's trust on destination D and n is the no. of hop. In the routing process, source broadcasts RREQ packet. When an intermediate node receives the first RREQ packet it checks the path list and hop count and updates its reverse route table and sets up reverse path. When duplicate request packet arrives at node it checks the hop count of that packet, if it has lesser hop count than the previous one, record of the previously received packet is replaced by the new one in the reverse route table. After receiving request packet destination node generates reply packet (RREP) and sends back to the sender. When an intermediate node receives RREP packet, it compares the trust value in RREP packet with the node's trust value from which it receives the RREP packet. If the node's trust value is less than the one in RREP packet, the trust value in RREP packet is replaced by that node's trust value. In this way, finally when RREP packet reaches to the source node, it gets the trust value from the RREP packet and set it as a trust value of that path. After receiving all the RREP packets and the path trust values, it sorts the paths based on the trust values. Then it breaks the message in three parts and encrypts it in the previously mentioned way and starts sending it to the appropriate path according to the data degree of secrecy. After route discovery, if the appropriate path is not found, routing process will be restarted.

4.9. Friend Based Ad Hoc Routing Using Challenges to Establish Security [16]

This algorithm achieves security in ad hoc network by sending challenges and sharing friend lists. In this scheme, there are different list of nodes:-

Question mark List: In this list, the nodes that are found to be suspicious by another node are recorded. Each and every node must have this list in its data structure.

Unauthenticated List: In this list totally unknown nodes are listed. The nodes in this list have no security information.

Friend List: the trusted nodes are listed here. These lists are also stored in data structure of every node. The rating of friends ranges from 0 to 10.

This algorithm has four steps: challenging neighbor, friends rating, sharing friends and route through friends. FACES is a hybrid protocol as the routing of data is on demand where as challenging and sharing occurs periodically. When the network is initialized, the nodes are not familiar with each other. So after initializing the network the nodes challenge each other to find the friend nodes. The challenging mechanism works as – suppose node A challenges its neighbor B. A first performs share Friend list with B by sending FREQ packet to B. After receiving FREQ packet from A, B replies by sending its all three list to A. After getting replies A picks one node (let C) from B's list to which it can reach by own. Then send a challenge packet to C directly and through node B. When C receives challenge packet it replies node A and node B in turns replies to node A. then node A compares these two results if it matches node A add B in its friend list otherwise in question mark list.
Friends are rated in this scheme using three parameters: Data rating (DR), friend rating (FR), net rating (NR). Initially the nodes only have friend List, nodes of which perform a successful challenge. The sharing of friend list takes place periodically. Let node B sends its friend list to node A during the friend sharing stage, then node A picks those nodes that are not in its own list from friend list of B and includes those nodes in its own list and the rating of those nodes, which is obtained from B set as FR of those nodes. The data rating (DR) of those nodes is set to zero. Then the net rating (NR) of node is calculated as:

$$NR=\frac{W1*DR+w2*FR}{w1+w2}$$

where w1 and w2 are the weight that is network dependent.
If the friend of B is already in the list of A i.e. if the nodes A and B have common nodes (let C) then A obtains rating of C from B and calculate obtain rating as:

OR= (net rating of B in list of A * net rating of C in list of B)/ 10

FR of node C is obtained by adding all OR from various neighbor nodes and divides the value by the sum of ratings of those various nodes. The data rating is calculated on the basis of data transfer by a node. DR is calculated as: $DR=10*(1-e^{-\lambda x})$, where x is no of forwarded data packets and λ is a factor by which data packets are related to rating. The routing of data takes place when any node has data to end. It broadcasts route request message including no of data it wants to send. After receiving route reply messages, it finds the best route depending on the net rating value of nodes, to the destination from its friend list. Then it sends data through that route and waits for back-off time. If any acknowledgement comes within back-off time DR increases. If not then it initiates sequential challenge to find malicious node that misbehaves.

4.10. Trust Based Security Protocol Routing [17]

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 n_k) receives packet from another node (let n_i), node nk increments the FC of ni as: $FCn_i=FCn_i+1$; i=1, 2…. Then this new FCni value is stored in NTT of node n_k. 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: - $SCn_i=FCn_i/Prec$, where Prec is the no of packets received at destination. This SCn_i is appended in RREP packet. The intermediate nodes in reverse path check the validity of the RREP packet by verifying digital signature of destination. If it is valid, the intermediate node signs the packet and forwards it to the next, otherwise the packet is dropped. When source node finally gets the reply it first verifies the first node id in RREP packet. If it is its neighbor, then all other intermediate nodes' digital signature is verified. If the verifications of all the nodes are successful then the trust counter is incremented for all the nodes as: Tci = Tci + δ1, if the verification is failed the trust counter value is decremented by 1: Tci = Tci - δ1.where δ1 is the small fractional value. The source node also checks the success ratio of all other nodes and compares it with the minimum threshold value (SRmin), if the SRni of a node is less than the SRmin the trust counter is decremented by another step value δ2 again, otherwise it is incremented. 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.

4.11. Trust Based DSR [18]

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. When a node receives any reply from its neighbor the trust value of neighbor node is updated. If any reply is not received by a node the trust value of the neighbor node is decreased. Trust value is evaluated as: $T= \tanh[(\Delta +W) *Te]$ 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, Δ is +1 for positive and 0 for negative experiences. Positive experience means acknowledgement is received within the time frame and otherwise it is considered as the negative experience. Administrator module keeps the trust information of all the known nodes and also has some methods to query this trust information. The monitor module monitors the received acknowledgments to adjust trust values of nodes. The router module selects the route to forward packets based on nodes trust values. Monitor module uses two routing strategy: In the first routing strategy, the route is rated based on the average value of all nodes along that path. The route which gets highest rating is selected for routing. In the second routing strategy, the average of all nodes trust value is divided by no of nodes to get shorter path. The route which gets high value is selected.

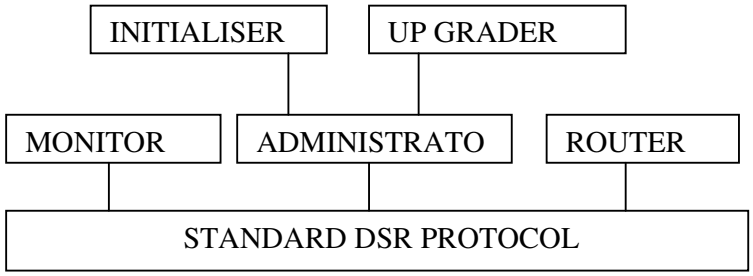

Figure 4. Components of TDSR

4.12. A Distributed Trust Management Framework for Detecting Malicious Packet Dropping Nodes in a Mobile Ad Hoc Network [19]

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. The trust mechanism is employed in this protocol by the communication among these modules. The modules work in the following way:

4.12.1. 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 etc. is noticed the node is marked as suspected node and the reputation collector module is invoked.

4.12.2. 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. On receiving the responses from its entire neighbor, the accused node calculates the group trust value which is calculated by the difference of absolute trust value and average value of degree of maliciousness and then sends back this value to the accuser node with all the responses that neighbor nodes send back to it.

4.12.3. 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 neighbour when it needs reputation value of itself .The neighbour nodes send back reply by sending rep_reply message to the accused node with reputation value of that node. A rep_broadcast message is sent to inform all other nodes when any malicious node is detected in the network.

4.12.4. Reputation Maintainer Module

A global trust state for all malicious nodes is maintained in a reputation table which has two field-node_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:

$$(1-T_{new})= \alpha\ (1-\ T_{old}) +\beta.(1-T_{certificate})-\delta$$

where T_{old} ,T_{new} and $T_{certificate}$ 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. Again $\beta=\alpha1.\ \alpha2.\ \alpha3$ where α2 is the weightage of new trust value computed and α1 and α2 are given by $\alpha1= (\sum\_majority[\![wi\ ti]\!])/W$ and $\alpha3= 1$ if $k\geq1$ where wi, ti are the weightage and trust value of the neighbours of accused node. W depends on the size of the network.

4.12.5. 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 neighbour nodes that are in 1-hop distance from the accused node. The neighbouring 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.

4.12.6. Alarm Raiser Module

The alarm raiser module starts to response when any malicious node is detected. The alarm message is flooded over the network to inform all other node in the network about the malicious node.

4.13. Reputated ARAN [20]

The ARAN protocol can't defend itself from authenticated selfish node that drop packets or do not participate in routing. The reputated ARAN scheme is proposed to defend against selfish nodes that do not forward packets to save its own resources. In this scheme, the nodes get incentives for their cooperation in routing. Initially all the nodes are assigned 0 value as a reputation value. This scheme has the following phases:

4.13.1. Route Lookup Phase

An authenticated route is established in this phase. If a node (let S) has data to send, it broadcasts route discovery packet (RDP) in the network which contains destination id, digital signature of S and certificate of S for authentication purpose. When any intermediate node receives the RDP packet, first it checks its routing table whether it has a route to the desired destination or not. If not then it appends its certificates to that packet and forwards the packet to its neighbour nodes and keeps an entry of that packet information in its routing table. This process is going on until the packet reaches to the destination node (let X). On receiving the all RDP packets node X replies with RREP packet corresponding to every RDP packets it received. The intermediate nodes forward the RREP packet in a reverse path using the information stored in routing table.

4.13.2. Data Transfer Phase

After getting several RREP packets for one RDP packet the source node select the path with high reputation. Then the source node sends data packets to that path and starts a timer. The destination node sends an acknowledgement (DACK) on receiving the data packets in reverse direction.

4.13.3. Reputation Phase

If acknowledgement of data packets comes within time out period the source node increment the reputation value of the next node by +1. And all the intermediate nodes also give +1 to its next hop node.

4.13.4. Time out Phase

In this phase, when the time out period of sent data packet expires the node gives negative recommendation of -2 to its next hop. The intermediate node also gives negative recommendation of -2 to its next hop when timer expires. The nodes delete the entry of that node from sent table. If the reputation of any node falls below threshold value -40 the node is rejected and sends an error message to the other nodes in that path.

5. COMPARISON OF DIFFERENT TRUST BASED ROUTING PROTOCOLS

Protocol	Advantage	Disadvantage
1. Dynamic Source Routing (DSR)	As DSR is a source based routing the intermediate node's need not to maintain any routing table, so network overhead is low. Source does not need to reinitiate the route discovery in	It is not a secure protocol because there is no mechanism for preventing attacks. It is not scalable to larger network. It requires more processing resources.

	case of link failure	
2. Ad Hoc On Demand Distance Vector (AODV)	1)Low end to end delay 2)Latest route discovery 3)Support unicast and multicast routing 4)No additional overheads 5)It is loop-free and scalable to large networks	1)Unicast routing for which heavy traffic load 2)Wastage of bandwidth 3)Vulnerable to various attacks created by malicious node 4)This protocol can't defend itself from selfish node
3. Trusted Ad Hoc on Demand Distance Vector (TAODV)	1)TAODV can detect malicious node and selfish node in network 2)It is more secure and having better performance than AODV 3)It can prevent modification, fabrication attacks	1)It has no authentication mechanism of nodes and messages 2)It can't prevent worm-hole and impersonation attack
4. Cooperation Of Nodes: Fairness In Dynamic Ad-Hoc Networks (CONFIDANT)	CONFIDANT protocol effectively detect selfish nodes and PM wormhole nodes that drop packets	1) It can't prevent various attacks such as modification impersonation fabrication Sybil attack by malicious nodes 2) An attacker is able to send false alarm messages and can do false claim that a node is misbehaving.
5.Ad Hoc On-Demand Trusted-Path Distance Vector(AOTDV)	Multiple loop free paths is established. Give the better performance in terms of packet delivery ratio, delay, packet overhead, path optimality in compare to AODV, AOMDV. It reduces grey-hole, black-hole attacks.	This protocol can't detect the nodes which do not drop packets. Just copy the packet and flood the network later to disrupt the routing procedure. In this protocol the source node need to overhear the network to know correct forwarding of packets. In case of limited battery power it is quite inefficient.
6.Friendship Based Ad Hoc On Demand Distance Vector (FrAODV)	This protocol gives better performance in terms of QoS services like packet delivery fraction, normalized routing load.	The end to end delay is not included in performance measurement metric. The delay is more here because two evaluation algorithms are used to establish path.
7.SecureRouting Using Trust(SRT):	In terms of mobile mobility it gives better throughput, packet delivery ratio, average path length, average routing load.	The performance decreases in the presence of attacks except black hole. The trust is calculated on the basis of control packets only.
8. Trusted AOMDV	Performance is measured in terms of route selection time,	This protocol measures the performance in fixed mobility

	trust compromise with TDSR,AOMDV etc	environment that actually not applicable in MANET.
9.Friend Based Ad Hoc Routing Using Challenges To Establish Security (FACES)	Challenge packet helps to detect flooding, grey-hole, spoofing, modification, dropping of control packets. As well as it gives better performance in the presence of malicious nodes.	In this protocol control overhead is increased due to periodic flooding of challenge packet and periodic sharing of friend list.
10. Trust Based Security Protocol(TMSP)	This protocol maintains confidentiality and authenticates the nodes based on digital signature. It detects the nodes which are misbehaving.	This protocol can't detect authenticated malicious node. In this protocol after finding route then the trust of the nodes along the path is calculated which increases control overhead. Because calculating the trust after finding path is inefficient as the path may be rejected due to presence of malicious nodes.
11. Trust Based DSR	It gives better throughput with general DSR.	This protocol doesn't consider delay, packet forward ratio, communication overhead matrices in performance analysis.
12. A Distributed Trust Management Framework For Detecting Malicious Packet Dropping Nodes In a Mobile Ad Hoc Network	This protocol detects malicious nodes which drops packet. It gives better performance in terms of false positive rate, successful detection rate, total convergence time and effective convergence time.	This protocol doesn't consider the nodes that do not drop packets. It doesn't consider the delay, throughput, packet deliver ratio when measures the performance.
13. Reputated ARAN	It can detect malicious node and selfish node in the network. It gives better performance than ARAN.	It does not consider the performance of the protocol in terms of QoS i.e. QoS metrics.

6. 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. Then we review currently existing trust based protocols and finally we have carried out a comparative study on these protocols on the basis of their merits and demerits.

In the above mentioned CONFIDANT protocol the attacker can send false alarm messages to isolate a good node by claiming it as a bad node. 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. These protocols only focus on the improvement of the performance through trust mechanisms but don't focus on the security flaws launched by malicious nodes on the network. Some protocols such as FrAODV, FACES increases communication overhead due to excessive calculation for route finding and periodic flooding of control packets.

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 behaviour without dropping packets and also authenticate the nodes to prevent attacks. So we can work on these disadvantages through implementing a new trust based protocol.

REFERENCES

[1] G. Aggelou (2004) Mobile Ad Hoc Networks, McGraw-Hill.

[2] N. Garg & R. P. Mahapatra, (2009) "MANET security issues" IJCSNS International Journal of Computer Science and Network Security, 9(8).

[3] M. Dasgupta, S. Choudhury & N. Chaki, (2010) "Routing Misbehaviour in Ad Hoc Network", International Journal of Computer Applications (0975 -8887).

[4] Supriya & M. Khari, (2012) "MANET Security Breaches: Threat to a Secure Communication Platform" , International Journal on Ad hoc Networking System(IJANS), Vol. 2, No. 2.

[5] S.J Lee, M. Gerla & C.K Toh, (1999) "A Simulation Study of Table-Driven and On-Demand Routing Protocols for Mobile Ad Hoc Networks", IEEE Network.

[6] D. B. Johnson, D. A. Maltz & Y.C. Hu, (2003) "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", IETF Draft.

[7] D. B. Johnson, D. A. Maltz, (1996) "Dynamic Source Routing in Ad Hoc Networks", Kluwer International Series in Engineering and Computer Science, 153-179.

[8] M. K. Marina, S.R. Das,(2001) "On-demand Multipath Distance Vector Routing in Ad-hoc Networks" In Network Protocols, Ninth International Conference on. IEEE, Pages 14-23.

[9] C. Perkins, E. Belding-Royer, S. Das, (2003) "Ad hoc on demand distance vector (AODV) routing", RFC 3561.

[10] A. M. Pushpa, (2009) "Trust based secure routing in AODV routing protocol", International Conference on Internet Multimedia Services Architecture and Applications (IMSAA), USA: IEEE Press, 1-6.

[11] S. Buchegger, J. L. Boudec, (2002) "Performance Analysis of CONFIDANT Protocol", MOBIHOC'02, EPFL Lausanne, Switzerland, pp226-236.

[12] X. Li. Jia, L. Wang, H. Wang, () "Trust based On demand Multipath Routing in Mobile Ad Hoc Networks", Information Security, IET, 4(4), 212-232.

[13] Essia, T., Razak, A., Khokhar, R.S., Samian, N.: Trust-Based Routing Mechanism in MANET: Design and Implementation. Springer, 18 June 2011.

[14] Edua Elizabeth, N., Radha, S., Priyadarshini, S., Jayasree, S., Naga Swathi, K.:SRT- Secure Routing using Trust Levels in MANETs. European Journal of Scientific Research, ISSN 1450-216X Vol. 75, No. 3 (2012), pp. 409-422

[15] 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

[16] Dhurandher, S.K., Obidant, M.S., Verma, K., Gupta, P., Dhuradar, P.:FACES: Friendhip-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems. IEEE SYSTEM JOURNAL, Vol.5, No. 2, June 2011
[17] Sharma, S., Mishra, R., Kaur, I.: New trust based security approach for ad-hoc networks .IEEE(2010)
[18] Bhalaji, N., Mukherjee, D., Banerjee, N., Shanmugam, A.:Direct Trust Estimated On Demand Protocol For Secured Routing In mobile Ad-Hoc Networks. International Journal of Computer Science & Security, Vol. 1, Issue (5)
[19] Sen, J.: 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
[20] 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

Authors

Mousumi Sardar has received her B.Tech degree in Information Technology in the year 2011 from College of Engineering & Management, Kolaghat, India. She is now perusing her M.Tech. degree in Information Technology from West Bengal University of Technology Kolkata, India.

Koushik Majumder has received his B.Tech and M.Tech degrees in Computer Science and Engineering and Information Technology in the year 2003 and 2005 respectively from University of Calcutta, Kolkata, India. He obtained his PhD degree in the field of Mobile Ad Hoc Networking in 2012 from Jadavpur University, Kolkata, India. Before coming to the teaching profession he has worked in reputed international software organizations like Tata Consultancy Services and Cognizant Technology Solutions. He is presently working as an Assistant Professor in the Dept. of Computer Science & Engineering in West Bengal University of Technology, Kolkata, India He has published several papers in International and National level journals and conferences. He is a Senior Member, IEEE.