Secured Routing through Multi Stage Authentication in MANETs

N.Madhuri1, B. Ananda Krishna2, Y.David Solomon Raju3
[1]*Student, M.Tech, DECS, Gudlavalleru Engineering College, Gudlavalleru,*
[2]*Professor, ECE Department, Gudlavalleru Engineering College, Gudlavalleru*
[3]*Assoc.Professor, Holy Mary Institute of Technology & Science, Hyderabad*

Abstract:
Mobile Ad Hoc Networks are characterized by the absence of fixed infrastructure, rapid topology change and high node mobility. These characteristics determine that wireless ad hoc network is more vulnerable to malicious attacks than the traditional Internet. Among many malicious attacks, a novel method is proposed to eliminate Black Hole attack. The proposed scheme is simple with low-overhead security mechanism during route discovery to secure the established route from potential attacks. The paper concludes that the proposed security model works well for heavily loaded networks with high mobility and can be extended to eliminate many other attacks.

Keywords
MANETS, Routing Security, Attacks, Authentication

1. Introduction

A Mobile Ad hoc Network (MANET) is a network composed only of nodes, with no access point. Messages are exchanged and relayed between nodes. In fact, an ad hoc network has the capability of making communications possible even between two nodes that are not in direct transmission range with each other. Packets to be exchanged between these two nodes are forwarded by intermediate nodes, using a routing algorithm. Hence, a MANET may spread over a larger distance, provided that its ends are interconnected by a chain of links between nodes (also called routers in this architecture).

1.1 Advantages and Disadvantages

The ad hoc networks are smaller in size with high speed multimedia services, more convenient and more powerful with device portability. The biggest ad hoc's strength is its independency from any infrastructure. Therefore, it is possible to establish an ad hoc network in any difficult situations. The following are the advantages of ad hoc networks.

- Infrastructure less and Low cost
- Mobility (MANET only)
- Decentralized and Robust
- Easy to Deploy
- Instant Infrastructure
- Disaster Relief
- Remote Areas
- Effectiveness

On the other hand, there are some drawbacks that need to be pondered:

- Hidden and Exposed Terminal Problems
- Limited Bandwidth
- Collisions
- Limited Power Source
- Security Problem
- Unpredictable Link Properties
- Sleep Period of Operation
- Looping Problem

2. Security in Ad hoc Networks

A Mobile Ad hoc Network consists of a set of mobile hosts that carry out basic networking functions like packet forwarding, routing, and service discovery without the help of an established infrastructure. Nodes of an ad hoc network rely on one another in forwarding a packet to its destination, due to the limited range of each mobile host's wireless transmissions. Security in MANET is an essential component for basic network functions like packet forwarding and routing: network operation can be easily jeopardized if countermeasures are not embedded into basic network functions at the early stages of their design. Unlike networks using dedicated nodes to support basic functions like packet forwarding, routing, and network management, in ad hoc networks those functions are carried out by all available nodes. This difference is at the core of the security problems that are specific to ad hoc networks [1].

Manuscript received October 5, 2014
Manuscript revised October 20, 2014

3. Attacks on Ad hoc Networks

3.1 Black Hole Attack

In this attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. The attacker will then receive the traffic destined for other nodes and can then choose to drop the packets to perform a denial-of-service attack, or alternatively use its place on the route as the first step in a man-in-the-middle attack by redirecting the packets to nodes pretending to be the destination.

3.2 Spoofing

A node may attempt to take over the identity of another node. It then attempts to receive all the packets destined for the legitimate node, may advertise fake routes, and so on. This attack can be prevented simply by requiring each node to sign each routing message (assuming there is a key management infrastructure). Signing each message may increase the bandwidth overhead and the CPU utilization on each node.

3.3 Modifying Routing Packets in Transit

A node may modify a routing message sent by another node. Such modifications can be done with the intention of misleading other nodes. For example, sequence numbers in routing protocols such as AODV are used for indicating the freshness of routes. Nodes can launch attacks by modifying the sequence numbers so that recent route advertisements are ignored. Typically it is particularly difficult to detect the node which modified the routing message in transit. Requiring each node to sign each routing message can prevent these types of attacks. In such a case, if a node modifies routing packets, then it might escape undetected, but it will not be able to mislead other nodes because the routing messages will not have the appropriate signature. Other nodes can detect illegal modifications in the packet via the cryptographic protection mechanisms.

3.4 Packet Dropping

A node may advertise routes through itself to many other nodes and may start dropping the received packets rather than forwarding them to the next hop based on the routes advertised. Another variation of this attack is when a node drops packets containing routing messages. These types of attacks are a specific case of the more general packet dropping attacks.

4. Related Works

Satoshi Kurosawa, et al., analyzed the black hole attack which is one of the possible attacks in ad hoc networks [2]. In order to prevent black hole attack, it is crucial to detect the abnormality occurs during the attack. In conventional schemes, anomaly detection is achieved by defining the normal state from static training data. However, in mobile ad hoc networks where the network topology dynamically changes, such static training method could not be used efficiently. In this paper, the authors proposed an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals.

In a Black hole attack, a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept [3]. To reduce the probability it is proposed to wait and check the replies from all the neighboring nodes to find a safe route. The approach is to combat the Black hole attack to make use of a 'Fidelity Table' wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a 'Black hole' and is eliminated. The authors proposed a solution Prevention of Co-operative Black Hole Attack (PCBHA) that is an enhancement of the basic AODV routing protocol, which will be able to avoid multiple black holes acting in the group.

Fei Wang, et al., proposed the Cooperative On-demand Secure Route (COSR) protocol to against the main passive route attacks [4]. COSR measures Node-Reputation (NR) and Route-Reputation (RR) by contribution, Capability of Forwarding (CoF) and recommendation to detect malicious nodes. Furthermore, COSR uses reputation to balance load to avoid hot-point in the network.

Hoang Lan Nguyen and Uyen Trang Nguyen presented Study of Different types of attacks on multicast in Mobile Ad Hoc Networks [5]. It is a simulation based study of the impacts of different types of attacks on mesh-based multicast in MANETs. They consider the most common types of attacks, namely rushing attack, black hole attack, neighbor attack and jellyfish attack. Specifically they studied how the processing delay of legitimate nodes, the number of attackers and their positions affect the performance metrics of a multicast session such as packet delivery ratio, throughput, end-to-end delay, and delay jitter.

Jieying Zhou, et al., presented SRSN: Secure Routing based on Sequence Number for MANETs to defend

against black hole attack [6]. This paper proposed a new method SRSN (Secure Routing based on Sequence Number) which based on the strict increment of sequence number of RREQ packet combined with reliable end to end acknowledgement to detect false route information. This paper discusses routing security issues of ad hoc network. They focus on black hole attack, which can be easily employed against ad hoc routing protocol.

Litu Jun, et al., presented a security enhanced AODV routing protocol based on the credence mechanism, which analyzes the potential insecurity factors in the AODV protocol [7]. A security routing protocol based on the credence model is proposed, which can react quickly when some malicious behaviors in the network are detected and effectively protects the network from kinds of attacks and guarantees the security of Ad Hoc networks. A security mechanism based on AODV protocol is proposed in this paper. It reinforces the protocol function, proposing AODV-AD (AODV with Attack Detection).

Michele N. Lima, et al., presented requirements for survivable routing in MANETS which suggest the cooperation among preventive, reactive and tolerant defense mechanisms as an approach to reach the survivability of essential services [8]. The authors highlighted survivability requirements for MANETs, and quantify the survivability of AODV and AOMDV protocols in the presence of black hole and selective forwarding attacks. The paper has discussed survivability requirements for MANETs, in order to support their goals in a timely manner, even in the presence of attacks and intrusions. Essential services for MANETs are highlighted and their requirements correlated.

Poly Sen, et al., proposed honesty-rate based collaborative intrusion detection for Mobile Ad-Hoc Networks [9]. This paper analyzes a new Honest-rate base collaborative Intrusion Detection System (HIDS) that has been proposed for mobile, ad-hoc networks. The method uses promiscuous mode of working along with rating and collaborative decision making based on multiple threshold values. All nodes join the network with an initial value of 1 for an honesty rate index, termed as h-rate. The h-rate of a node dynamically increases or decreases depending on its behavior. A node is rewarded when it forwards packets for other nodes. It is penalized when it does some malicious act like dropping packets, etc. The h-rate for a node is recomputed based on its current h-rate, and the rewards or penalty points that it has accrued.

Satish Salem Ramaswami and Shambu Upadhayaya proposed a new method of handling of colluding black hole attacks in MANETs and Wireless Sensor Networks using multiple path Routing [10]. They addressed the problem of colluding and coordinated Black hole attacks, one of the major security issues in MANET based defense application. This paper mainly based on the reducing the overhead in the network.

5. Security Mechanism

We provide a framework for avoiding Black hole attack in the Ad hoc On-demand Distance Vector (AODV) routing protocol. We have designed the mechanism that will ensure the proper data packet transmission and reception between the source and destination.

5.1 Route Discovery Process in AODV

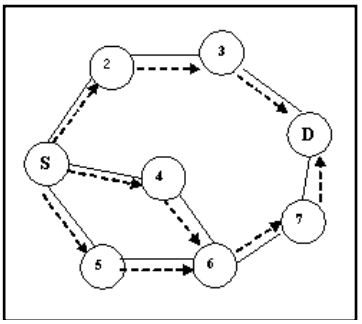

Fig. 1: Route Discovery Process

When a node needs to determine a route to a destination node, it floods the network with RREQ packets. The originating node broadcasts a RREQ packet to its neighboring nodes, which broadcast the packet to their neighbors, and so on as shown in figure 1. As these requests spread through the network, intermediate nodes store reverse routes back to the originating node. Since an intermediate node could have many reverse routes, it always picks the route with the smallest hop count.

When a node receiving the request either knows of a "fresh enough" route to the destination or is itself the destination, the node generates a RREP packet, and sends this packet along the reverse path back towards the originating node as shown in the figure 2. As the RREP packet passes through intermediate nodes, these nodes update their routing tables, so that in the future, packets can be routed through these nodes to the destination. Notice that it is possible for the RREQ originator to receive a RREP packet from more than one node. In this case, the RREQ originator will update its routing table with the most "recent" routing information; that is, it uses the route with the greatest destination sequence number.

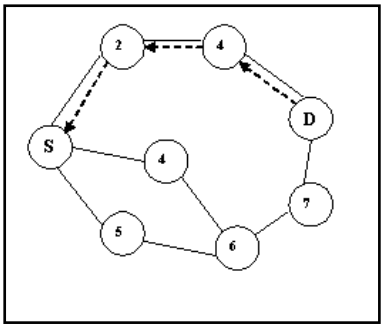

Fig.2: Propagation of RREP Packet

5.2 Black Hole Problem in AODV

Consider an Ad Hoc Network in which the Source node (1) wants to send data packets to the Destination node (6). The Intermediate node (3) is assumed to be a Black Hole with no fresh enough route to node 5. Before transmitting the data packets, the node 1 initiates a Route Discovery Process as shown in the figure 3.

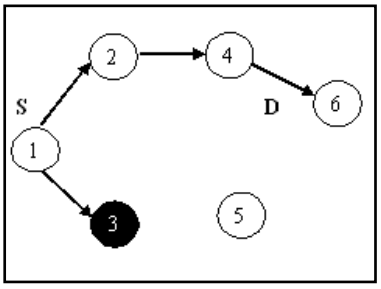

Fig. 3: Route Discovery Process

As node 3 is a Black Hole, whenever it receives a RREQ packet, it immediately sends a RREP packet stating that it has the shortest route to the destination node as shown in the figure 4.

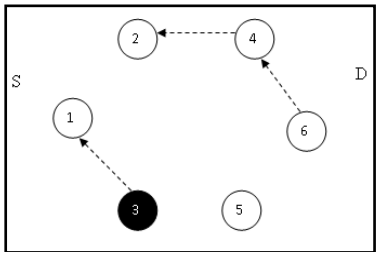

Fig.4: Propagation of RREP Packet

If the reply from a normal node reaches the source node of the RREQ packet first, everything works well; but the reply from node 3 could reach the source node first, since it is nearer to the source node. Moreover, a Black Hole does not need to check its routing table when sending a false message; its response is more likely to reach the source node first. This makes the source node to think that the route discovery process is complete, ignore all other reply packets, and begin to send data packets as shown in the figure 5. As a result, all the packets through the black hole are simply consumed or lost. This problem is called as the "Black Hole Problem" and in this way the Black Hole can misroute a lot of network traffic to it, and could cause an attack to the network.

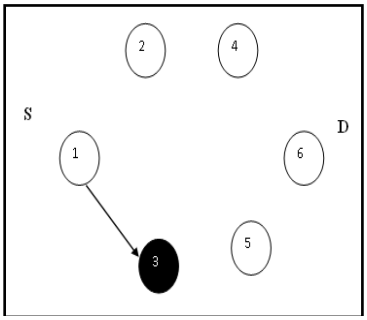

Fig. 5: Transmission of Data Packets

6. Solution

To prevent the Black hole attack and to achieve secure route in MANETs, the network requires to provide authentication and digital signatures for the control packets; that is, any node that receives a request or reply packet must be able to ascertain that the claimed initiator sent it. An authentication protocol should be lightweight and impose as small computational and message overhead as possible due to the fact that resources in a mobile ad hoc network are very limited. The proposed scheme, have used one's complement and RSA algorithm for securing the route.

In our proposed method, authentication at two stages is implemented. Before sending a RREQ message, every node in the network is required to append the one's complement of its own IP address as first level and the originator signs the destination IP address with public key at the second level. The node receiving the packet checks the authentication of its source by adding the appended one's complement and the source IP address known to it to get all ones but cannot decrypt the cipher text. Any malicious node sneaking into the network does not know that it has to append the one's complement of its IP address and thus any packet from such nodes get dropped by its neighbors. Also, once a node fails the test for authenticity, a broadcast is made to the whole network, warning all the nodes in the network of the presence of a malicious node and its IP address. This saves processing time, as any node receiving any packet

from the malicious node can simply discard it without any further checking. Thus the malicious node is isolated from the network. After the RREQ reaches the destination node, the destination decrypts with its private key and checks the integrity of the source and destination IP addresses. If the objects have been altered during transmission, the destination node will raise an alarm. Otherwise, it generates RREP packet, along with the digital signature and sends it back to the originator of the request. The originator will verify the authentication and integrity upon receiving the RREP packet from the destination. The hop to hop authentication is shown in the figure 6 and in algorithm 1.

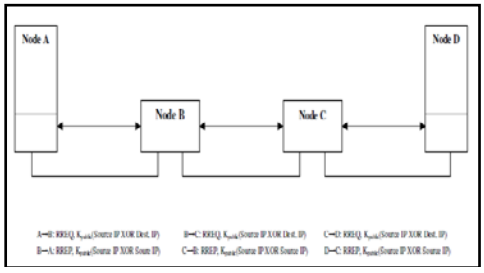

Figure 6: Hop to Hop authentication

A→B→C→D

- *Find the 1's complement of node's IP address*
- *Let (Soure IP XOR Dest.IP XOR) = XYZ*
- *A sends RREQ by encrypting XYZ with public key, K_{public}*
- *Switch on Timer and transmit RREQ packet*
- *(RREQ,Cipher) is transmitted to neighboring nodes*
- *Neighboring nodes verify IP address by appending 1's complement and forward RREQ to the destination node*
- *The node B can verify the RREQ, but fails to decrypt the cipher text, and sends to node C*
- *Similarly, node C can verify the RREQ, but fails to decrypt the cipher text*
- *Finally, the destination node receives the RREQ and decrypts the cipher text with its private key*
- *Plain text, $XYZ = C^e \pmod n$*
- *Performs XYZ XOR Dest.IP gives Source IP*
- *Verifies the Source and Destination IP addresses mentioned in the RREQ*
- *If they match, the destination D encrypts the RREP and retransmits to Source node through neighboring nodes*
- *Otherwise D raise the alarm to neighboring nodes*

Algorithm 1: Identification of malicious nodes

Along with the one's complement of IP address, we also install a TIMER in all the nodes. The Timer is switched ON when a RREQ packet is sent and the Timer is switched OFF when a RREP packet is received by the same node. Thus, the Timer's value denotes the time for receiving a Route Reply from its neighboring node. As the Black Holes immediately reply without checking the routing table and one's complement of IP address, the IP address doesn't matches and the Timer's value will be less when compared with a normal node. But the Timer's value will also be less when the destination node is nearer to the source node. To avoid this problem, the Timer's value is compared with the Threshold value. The Threshold value is the time required for receiving the route reply from a normal node. If the Timer's value is lesser than the Threshold value, then the node, which sent the RREP packet, is assumed to be a Black Hole. The strength of the proposed algorithm lies in

- Simple authentication at two different stages
- Without the knowledge of one's complement the malicious nodes can reply immediately lesser than the threshold value.

The algorithm for identification of malicious nodes and possible acts of the malicious nodes are given in the algorithm 2 and 3.

- *Assume that malicious node enters the network*
- *Receives the RREQ packet and sends RREP immediately acting as the destination without appending the 1's complement of IP address*
- *RREP receives by a particular node confirms that it was sent by the malicious node*
- *Immediately raise the alarm to the neighboring nodes*

Algorithm 2: Malicious nodes without the knowledge of 1's complement

- *Assume that malicious node enters the network*
- *Receives the RREQ packet and appends 1's complement on IP address and sends the RREP immediately acting as the destination*
- *Source node calculate the receiving time and compares with the threshold value*
- *Also source node checks for the authentication by decrypting the RREP packets and if it found the authentication fails, it arise alarm to the neighboring nodes.*
- *And also, if the calculated time < threshold value, confirms as malicious*
- *If the calculated time > threshold value and authentication proves, source node has yet to confirm*

Algorithm 3: Malicious nodes with the knowledge of 1's complement

To confirm the node to be a Black Hole, we do the following process.

6.1 Further Request

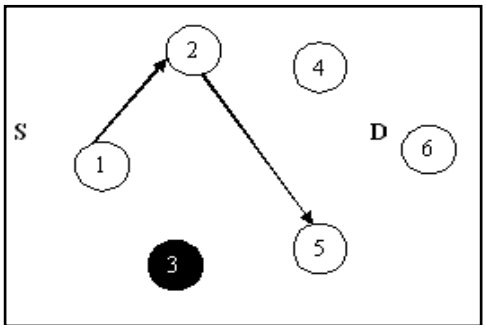

Fig. 7: Transmission of Further Request

In the proposed method, we require each intermediate node to send back the next hop information when it sends back a RREP packet. Thus, node 3 sends back the next hop information when it sends the RREP packet to source node 1. Here we assume the next hop it sends back is node 5. When node 1 receives the RREP packet from node 3, it does not send the data packets right away, but extracts the next hop information from the reply packet and then sends a Further Request to the next hop (node 5 as shown in the figure 7 to verify that it has a route to the intermediate node which sent the RREP packet, and that it has a route to the destination node. In response to the Further Request, the inquired intermediate node sends back a Further Reply as shown in figure 8.

6.2 Further Reply

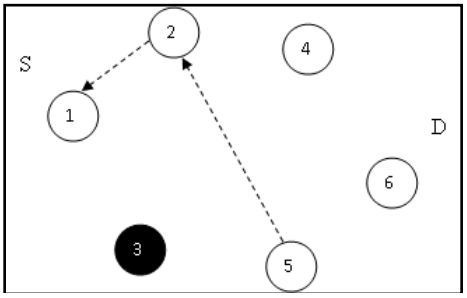

Fig. 8: Transmission of Further Reply

To avoid the problem of recursiveness, only the requested next hop can send back a Further Reply packet, which includes a Check Result. When the source node receives the Further Reply from the next hop, it extracts the Check Result from the reply packet. The Check result may be of three types as follows as given in table 1:

Table 1: Values of Check Result

Check Result	Explanation
1	Intermediate node is a Black Hole
2	Intermediate node is not a Black Hole
3	Initiate a new Route Discovery Process

7. Advantages

Our security mechanism scores over others by the fact that it is a very simple form of authentication avoiding complex cryptographic calculations reducing the processing overhead on the intermediate nodes. The incorporation of the signature in the control packet level greatly reduces the delay. Moreover, the novelty of our scheme, as compared with other MANET secure routing schemes, is that false route replies, as a result of malicious node behavior, are discarded by benign nodes while in-transit towards the querying node, or deemed invalid upon reception. Our security scheme takes care of most of the types of malicious attacks.

8. Simulation Parameters

The performance of the proposed security model is evaluated using the GloMoSim. Mobile nodes move in an unobstructed plane following the random waypoint model in which the node selects a destination randomly within the simulated territory, moves to that

destination as speed uniformly distributed in (Vmin, Vmax) m/s and stops there for a predefined pause time and then repeats this behavior for the entire duration of the simulation. The simulation is done for a network having 50 mobile nodes, which move over an area of 1000 x 1000 m2 with a certain speed. Table 2 gives the system parameter values used in the analysis and simulations.

Table 2: Simulation Parameters

Simulation Time	10 Min
Bandwidth	2 Mbps
Frequency of Operation	2.4 GHz
Simulation Area	1000 m x 1000 m
Number of Nodes	50
Offered Traffic	12 packets/sec
Radio Range	250 meters
Application	CBR
Transport	TCP
Network	AODV
MAC	802.11

8.1 Simulation Results

The following figure summarize the performance results of routing security with respect to total overhead obtained using GloMoSim by comparing with different speed and different number of nodes, is presented.

Total overhead: Measured as the ratio of the total packets transmitted (i.e., sum of control packets and data packets) to the data packets delivered.

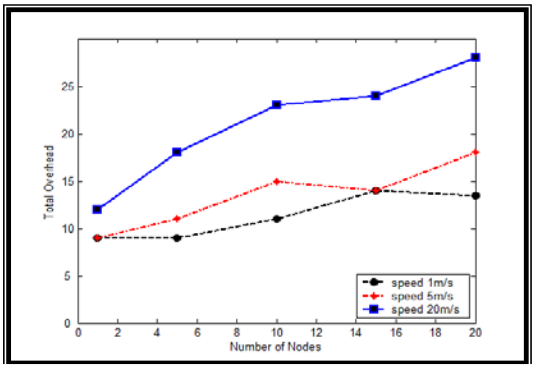

Fig. 9: Total Control Overhead Vs Number of Nodes

Figure 9 shows the total control overhead vs. Number of Nodes and it is observed that the number of total control overhead is small for lower speed and increases to 64% more for higher speed than with low mobility as the traffic in the network increases from 1 to 20. This is due to the number of route failures increase as the speed of the node increases from 1m/s to 20m/s, which in turn increases the number of route discovery process.

9. Conclusion and Future work

A novel method for the routing security in Mobile Ad hoc Network using simple cryptographic algorithms is discussed. The proposed methodology was investigated on the performance of AODV with CBR traffic. The protocol performance with routing security is analyzed and observed that total control overhead is small for lower speed and increases to 64% more for higher speed than with low mobility as the traffic in the network increases from 1 to 20. As a future work, the proposed algorithm is to be analyzed with respect to delay, speed and strength of the proposed algorithm.

References

[1] Y. Zhang, W. Lee, “Intrusion Detection in Wireless Ad Hoc Networks”, Proceedings of MobiCom, Boston, MA, pp. 275-283, 2000

[2] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, “Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method”, International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007

[3] Latha Tamilselvan and V Sankaranarayanan, “Prevention of Co-operative Black Hole Attack in MANET”, Journal Of Networks, Vol. 3, No. 5, May 2008

[4] Fei Wang, Yijun Mo and Benxiong Huang, “COSR: Cooperative On-Demand Secure Route Protocol in MANET” , IEEE ISCIT, pp.890-893, 2006

[5] Hoang Lan, Nguyen uyen, Trang Nguyen, “Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks”, Proceedings of the International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, IEEE Computer Society, 2006

[6] Jieying Zhou, Junwei Chen and Huiping Hu, “SRSN: Secure Routing based on Sequence Number for MANETs” IEEE Paper, pp.1569-1572, May 2007

[7] Litu Jun, Li Zhe and Lin Dan Liu Ye, “A security Enhanced AODV Routing Protocol Based on the Credence Mechanism”, IEEE, pp.719-722, 2005

[8] Michele N. Lima, Helber W. da Silva, Aldri L. dos Santos and Guy Pujolle, “Requirements for survivable routing in MANETS”, IEEE, pp 441-445, 2008

[9] Poly Sen, Nabendu Chaki and Rituparna Chaki, “Honesty-rate based Collaborative Intrusion Detection for Mobile Ad-Hoc Networks”, Proceedings of 7th computer Information Systems and Industrial Management Applications, IEEE Computer Society, pp. 121-126, 2008

[10] Satish Salem Ramaswami and Shambhu Upadhayaya “Smart Handling of Colluding Black hole Attacks in MANETs and Wireless Sensor Networks using Multipath Routing”, Proceedings of IEEE Workshop on Information Assurance, pp. 253-260, 2006