INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

SECURE DYNAMIC SOURCE ROUTING IN MOBILE ADHOC NETWORKS

Pooja Sharma[1], Seep Sethi[2]

[1]M.Tech (ECE), [2]Head of ECE Department
Somany (PG) Institute of Technology & Management, Rewari

Abstract: *A mobile ad-hoc network is a self-configuring network or infrastructure-less network of mobile nodes connected by wireless links which together form a random topology. Due to absence of centralized control, multi-hop communications and dynamic network topology, the provision of making routing secure in mobile ad hoc networks is much more challenging than the security in wired network or infrastructure based networks. Nodes in mobile Ad Hoc Network (MANET) do not depend on a central infrastructure but relay packets originated by other mobile nodes. Mobile ad hoc networks can work properly only if the participating nodes cooperate in routing and forwarding. For individual nodes it might be advantageous not to cooperate, though. In this research paper, we propose a new approach based on relationship among the mobile nodes which makes them to cooperate in an infrastructure-less environment. The faith unit is used to calculate the faith values of each node in the network. The calculated faith values are being used by the relationship estimator to determine the relationship status of mobile nodes. The proposed enhanced protocol was compared with the standard DSR protocol and the results are analyzed using the MATLAB-R2008a.*

1. INTRODUCTION

1.1 DSR Protocol

DSR is a source routing in which the source node starts and take charge of computing the routes [1]. At the time when a node S wants to send messages to node T, it firstly broadcasts a route request (RREQ) which contains the destination and source nodes' identities. Each intermediate node that receives RREQ will add its identity and rebroadcast it until RREQ reaches a node n who knows a route to T or the node T. Then a reply (RREP) will be generated and sent back along the reverse path until S receives RREP. When S sends data packets, it adds the path to the packets' headers and starts forwarding. During route maintenance, S detects the link failures along the path. If it happens, it repairs the broken links. Otherwise, when the source route is completely broken, S will restart a new discovery. Route discovery process in general is shown in fig. 1. To initiate the Route Discovery [2], the source transmits a ROUTE REQUEST (RREQ) message as a single local Broadcast packet, which is received by (approximately) all nodes currently within wireless transmission range of source. Each RREQ message identifies the initiator and target of the Route Discovery, and also contains a *unique request id,* determined by the initiator of the REQUEST. Each RREQ also contains a record listing the address of each intermediate node through which this particular copy of the RREQ message has been forwarded. This route record is initialized to an empty list by the initiator of the Route Discovery. When another node receives a RREQ, if it is the target of the Route Discovery, it returns a ROUTE REPLY (RREP) message to the initiator of the Route Discovery, giving a copy of the accumulated route record from the RREQ; when the initiator receives this ROUTE REPLY, it caches this route in its Route Cache for use in sending subsequent packets to this destination.

Otherwise, if this node receiving the RREQ has recently seen another RREP message from this initiator bearing this same request id, or if it finds that its own address is already listed in the route record in the RREQ message, it discards the REQUEST. Otherwise, this node appends its own address to the route record in the ROUTE REQUEST message and propagates it by transmitting it as a local broadcast packet with the same request id. Route Maintenance [3] is the mechanism by which source node is able to detect, while using a source route to destination node, if the network topology has changed such that it can no longer use its route to destination node because a link along the route no longer works. When Route Maintenance indicates a source route is broken, source node can attempt to use any other route it happens to know to destination node, or can invoke Route Discovery again to find a new route. Route Discovery and Route Maintenance each operate entirely *on demand.*

Volume 4, Issue VI, June 2016
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

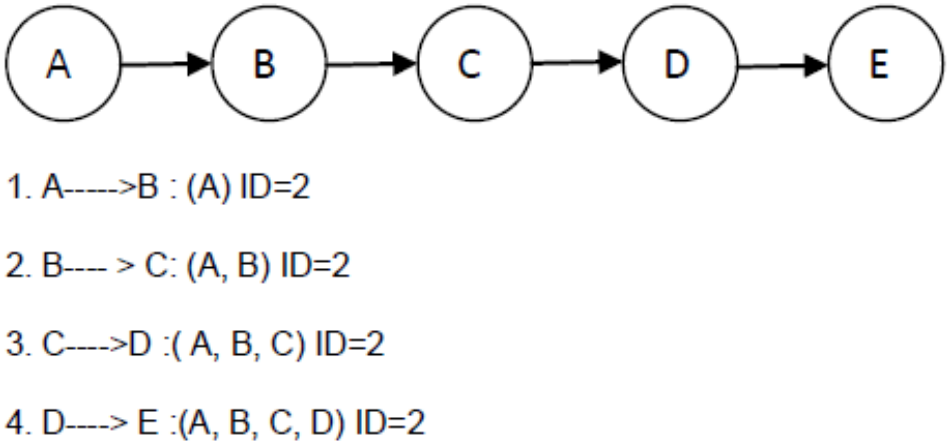

Figure 1: Route Discovery process

For example, DSR does not use any periodic routing advertisement, link status sensing, or neighbor detection packets, and does not rely on these functions from any underlying protocols in the network. This entirely on-demand behavior and lack of periodic activity allows the number of overhead packets caused by DSR to scale all the way down to zero, when all nodes are approximately stationary with respect to each other and all routes needed for current communication have already been discovered. As nodes begin to move more or as communication patterns change, the routing packet overhead of DSR *automatically* scales to only that needed to track the routes currently in use. In response to a single Route Discovery (as well as through routing information from other packets Overheard), a node may learn and cache multiple routes to any destination[4]. This allows the reaction to routing changes to be much more rapid, since a node with multiple routes to a destination can try another cached route if the one it has been using should fail. This caching of multiple routes also avoids the overhead of needing to perform a new Route Discovery each time a route in use breaks. When originating or forwarding a packet using a source route, each node transmitting the packet is responsible for confirming that the packet has been received by the next hop along the source route; the packet is retransmitted (up to a maximum number of attempts) until this confirmation of receipt is received. For example, in the situation illustrated in Fig. 1, node A has originated a packet for E using a source route through intermediate nodes B, C and D. In this case, node A is responsible for receipt of the packet at B, node B is responsible for receipt at C, node C is responsible for receipt at D, and node D is responsible for receipt finally at the destination E. This confirmation of receipt in many cases may be provided at no cost to DSR, either as an existing standard part of the MAC protocol in use such as the link-level acknowledgement frame defined by IEEE 802.11 or by a *passive acknowledgement.* If neither of these confirmation mechanisms are available, the node transmitting the packet may set a bit in the packet's header to request a DSR-specific software acknowledgement be returned by the next hop; this software acknowledgement will normally be transmitted directly to the sending node, but if the link between these two nodes is uni-directional, this software acknowledgement may travel over a different, multi-hop path. If the packet is retransmitted by some hop the maximum number of times and no receipt confirmation is received, this node returns a ROUTE ERROR message to the original sender of the packet, identifying the link over which the packet could not be forwarded. For example, in Fig. 2, if C is unable to deliver the packet to the next hop D, then C returns a ROUTE ERROR to A, stating that the link from C to D is currently "broken." Node A then removes this broken link from its cache; any retransmission of the original packet is a function for upper layer protocols such as TCP[5]. For sending such a

retransmission or other packets to this same destination E, If A has in its Route Cache another route to E (for example, from additional ROUTE Replies from its earlier Route Discovery, or from having overheard sufficient routing information from other packets), it can send the packet using the new route immediately. Otherwise, it may perform a new Route Discovery for this target.

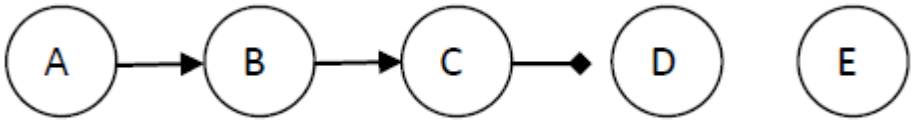

Figure 2: Route Maintenance Process

The operation of Route Discovery and Route Maintenance in DSR are designed to allow uni-directional links and asymmetric routes to be easily supported. In particular, in wireless networks, it is possible that a link between two nodes may not work equally well in both directions, due to differing antenna or propagation patterns or sources of interference. DSR allows such uni-directional links to be used when necessary, improving overall performance and network connectivity in the system [3]. DSR also supports internetworking between different types of wireless networks, allowing a source route to be composed of hops over a combination of any types of networks available. A node forwarding or overhearing any packet may add the routing information from that packet to its own Route Cache. In particular, the source route used in a data packet, the accumulated route record in a ROUTE REQUEST, or the route being returned in a ROUTE REPLY may all be cached by any node [6].

1.2 Black Hole Attack

In a black hole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example, in DSR, the attacker can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic. As for gray hole, its behavior is similar to a black hole[7]. A gray hole does not drop all data packets but just part of packets. We define the *Gray Magnitude* as the percentage of the packets which are maliciously dropped by an attacker [4]. For example, a gray hole is gray magnitude of 60% will drop a data packet with a probability of 60% and a classical black hole has a gray magnitude of 100%. Fig. 3 shows an example of a black hole attack, where attacker A sends a fake RREP to the source node S, claiming that it has a sufficiently fresher route than other nodes. Since the attacker's advertised sequence number is higher than other node's sequence numbers, the source node S will choose the route that passes through node A.

1.3 Challenges in MANET

In a mobile ad hoc network, all the nodes cooperate with each other to forward the packets in the network, and hence each node is effectively a router. Thus one of the most important issues is routing[8]. This thesis focuses mainly on routing issues in ad hoc networks. In this section, some of the other issues in ad hoc networks are described:

i) Distributed network: A MANET is a distributed wireless network without any fixed infrastructure [7]. That means no centralized server is required to maintain the state of the clients.

ii) Dynamic topology: The nodes are mobile and hence the network is self-organizing. Because of this, the topology of the network keeps changing over time [6]. Consequently, the routing protocols designed for such networks must also be adaptive to the topology changes.

iii) Power awareness: Since the nodes in an ad hoc network typically run on batteries and are deployed in hostile terrains, they have stringent power requirements [9]. This implies that the underlying protocols must be designed to conserve battery life.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

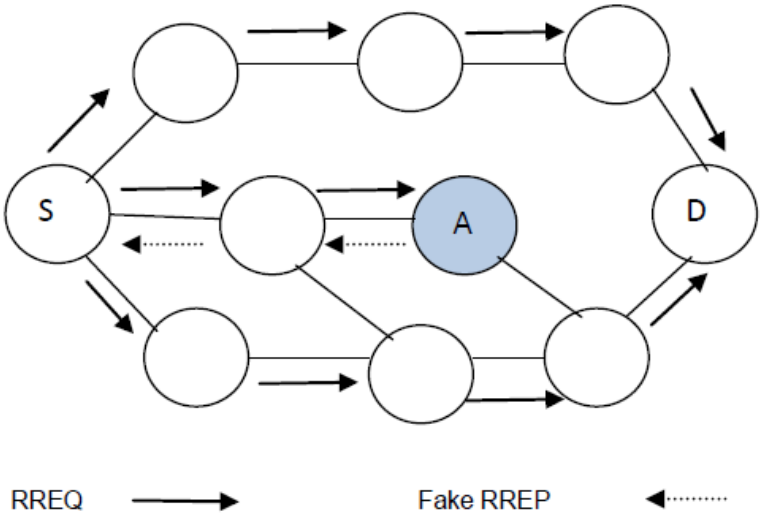

Figure 3: Example of a Black Hole Attack on DSR.

iv) *Addressing scheme:* The network topology keeps changing dynamically and hence the addressing scheme used is quite significant. A dynamic network topology requires a ubiquitous addressing scheme, which avoids any duplicate addresses. In wireless WAN environments, Mobile IP [10] is being used. Because the static home agents and foreign agents are needed, hence, this solution is not suitable for ad hoc network.

v) Network size: The ability to enable commercial applications such as voice transmission in conference halls, meetings, etc., is an attractive feature of ad hoc networks. However, the delay involved in the underlying protocols places a strict upper bound on the size of the network.

vi) Security: Security in an ad hoc network is extremely important in scenarios such as a battlefield [8]. The five goals of security – availability, confidentiality, integrity authenticity and non-repudiation - are difficult to achieve in MANET, mainly because every node in the network participates equally in routing packets.

2. PROPOSED METHODOLOGY

1. Here we are proposing a secure routing technique to deliver the data packets from source to destination.
2. In this technique, we have added nodes faith values according to its cooperation in delivering data packets.
3. For each node in the network, a faith value will be stored that represent the value of the faithfulness to each of its neighbor nodes. We will supply this value to each and every node in the network.
4. It will range from 0.1 to 1. 0.1 faith value means that the node will be preferred least to transfer data packets from source to destination. 0.1 faith value also indicates that the node is a malicious node that can harm the packet. 0.2, 0.3 indicates that these are selfish nodes and 1 indicates that the node will definitely transfer data packets. If a node starts transferring data to neighbour nodes, then the faith value of that node will be incremented by 0.1.
5. We have applied dijkstra algorithm to find out the shortest route or path from source to destination.
6. We have supplied three input parameters to dijkstra algorithm. Source node, Destination node and nodes faith values.
7. We can calculate shortest path based on faith values and total distance or cost by using Dijkstra algorithm.

3. IMPLEMENTATION & RESULTS

The simulation was carried out in MATLAB R2008a. Simulation parameters are shown in table 1. We have 10 nodes for simulation and traffic type is random waypoint, where percentage of malicious

Volume 4, Issue VI, June 2016
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

node is 10% i.e. one node will act as blackhole in this simulation. The area for simulation is 50 m X 50 m. The assumptions are node 1 will act as source and node 10 will act as destination, whereas node 9 will act as blackhole.

Table 1: Simulation Parameters

Number of Nodes	30
Terrain dimension	100 m x100 m
Traffic Type	Random waypoint
Simulation Rounds	100
# malicious nodes	1
MAC protocol	IEEE 802.11

Figure 4 have showed the process of route selection in DSR routing protocol. Route selection through blackhole node is shown in figure 5. Figure 6 and figure 7 have showed the route selection process of Secure-DSR by avoiding blackhole node from route selection process. Figure 8 have showed the comparison between Secure-DSR and DSR routing technique in terms of packet sent to destination without interception though black hole. Figure 9 have showed the comparison between Secure-DSR and DSR routing technique in terms of packet sent to destination with interception through blackhole.

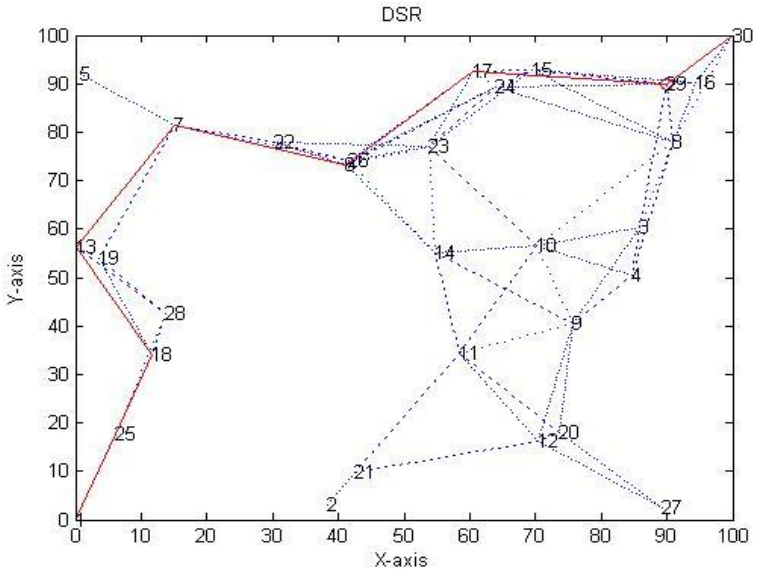

Figure 4: DSR route selection process

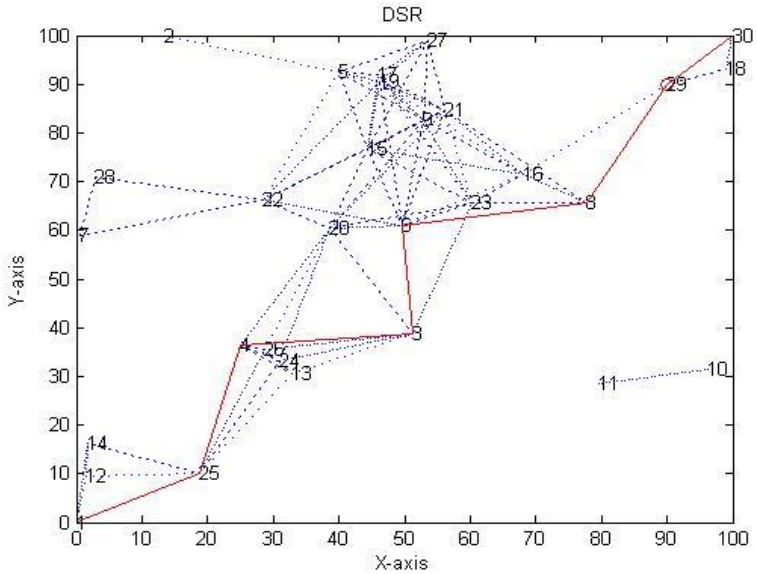

Figure 5: DSR route selection through blackhole node

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

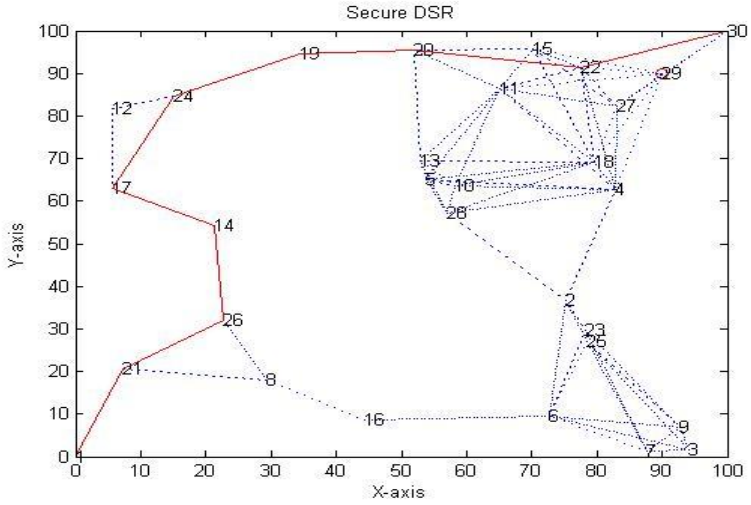

Figure 6: Secure DSR route selection process

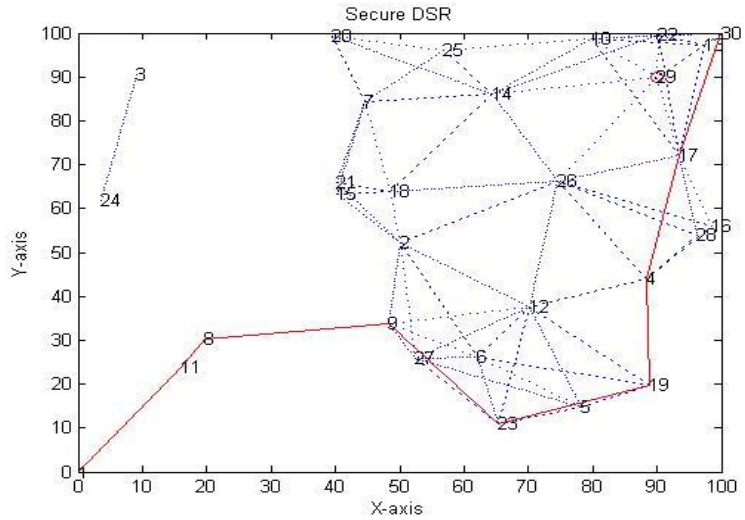

Figure 7: Secure DSR route selection process

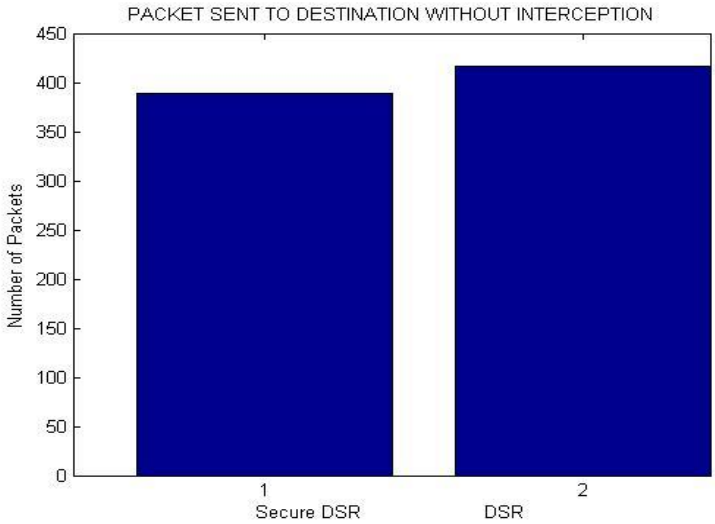

Figure 8: Packet sent to destination without interception though black hole

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

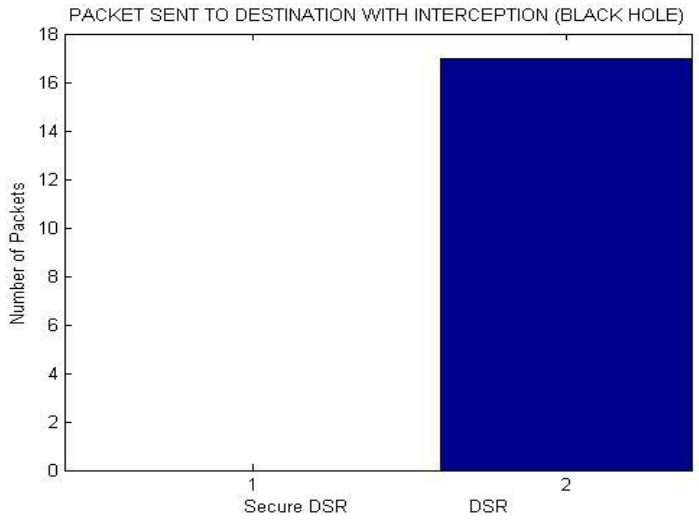

Figure 9: Packet sent to destination with interception through black hole

4. CONCLUSION AND FUTURE WORK

Secure routing protocols is a crucial area towards security of MANET. The routing solutions for conventional networks are not sufficient to work efficiently in ad-hoc environment. In this dissertation, we have proposed a scheme to select secure route for data forwarding. This technique will avoid interception of messages through black hole nodes. We have compared our results with DSR routing protocol, the results showed that Secure DSR will avoid routing of packets through black hole nodes. The goal of this work is to provide a simple node based trust management scheme for MANET with multiple perspectives on the concept of trust, an understanding of the properties, which should be considered in developing a trust metric, and insights on how a trust metric can be customized to meet the requirements and goals of the NTM scheme. The model is simple, flexible and easy to be implemented.

After introducing and analyzing the concept of node-based trust in MANET, we suggested future research directions to develop trust management schemes with desirable attributes such as adaptation to environmental dynamics, scalability and reliability.

REFERENCES

[1]. P Narayan, V R. Syrotiuk,"Evaluation of the AODV and DSR Routing Protocols Using the MERIT Tool", InIn proceeding or ADHOC-NOW 2004, pp25-36

[2]. K.Selvavinayaki, K.K.Shyam Shankar, Dr.E.Karthikeyan "Security Enhanced DSR Protocol to Prevent Black Hole Attacks in MANETs" ***International Journal of Computer Applications (0975 – 8887)*** **Volume 7– No.11, October 2010.**

[3]. Li, Xin; Jia, Zhiping; Wang, Haiyang;"Trust-based On-demand Multipath Routing in Mobile Ad Hoc Networks" IET Information Security, 2012 .

[4]. Sun, Y., Yu, W. ,Han, Z.,and Liu, K.J.R.:'Information Theoretic Framework of Trust Modeling and Evaluation for AdHoc Networks', IEEE Journal on Selected Areas in Communications, 2006, 24, (2),pp. 305-317

[5]. G. Theodorakopoulos and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks," ***IEEE J. Sel. Areas Commun.*****, vol. 24, no. 2, pp. 318-328, Feb. 2006.**

[6]. M. E. G. Moe, B. E. Helvik, and S. J. Knapskog, "TSR: Trust-based Secure MANET Routing using HMMs," ***Proc. 4th ACM Symposium on QoS and Security for Wireless and***

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

***Mobile Networks*, Vancouver, British Columbia, Canada, 27-28 Oct. 2008, pp. 83-90.**

[7]. Y. L. Sun, W. Yu, Z. Han, and K. J. R. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, Feb. 2006, pp. 305-317.

[8]. V. Balakrishnnan, V. Varadharajan, U. K. Tupakula, and P. Lucs, "Trust and Recommendations in Mobile Ad Hoc Networks," *Int'l Conf. on Networking and Services*, Athens, Greece, 19-25 June 2007, pp. 64-69.

[9]. S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *Proc. 6th Annual ACM/IEEE Mobile Computing and Networking*, Boston, MA, Aug. 2000, pp.255- 265.

[10]. J. Sen, P. Chowdhury, and I. Sengupta, "A Distributed Trust Mechanism for Mobile Ad Hoc Networks," *Int'l Symposium on Ad Hoc and Ubiquitous Computing*, 20-23 Dec. 2006. Surathkal, India, pp. 62-67.