Faith based Routing in Mobile Ad Hoc Network

Rohini Jatana
M.Tech scholar(ECE)
ECE Department
PIET,Samalkha

Rajesh Kumar
Assistant professor
ECE Department
PIET,Samalkha

ABSTRACT
MANET is a collection of wireless mobile nodes that work together by forwarding packets for each other to let them to communicate outside the range of direct wireless transmission or with each other. Secure routing protocols are 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 work, 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 Faith 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, 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 network trust management scheme. The model is simple, flexible and easy to be implemented. The proposed routing protocol is compared with DSR protocol and the results are analyzed using the MATLAB.

Keywords
Manet, secure DSR, secure routing, faith based DSR, blackhole

1. INTRODUCTION

1.1 Mobile Ad Hoc Network
Mobile Ad Hoc network is a set of wireless mobile nodes: that work together by forwarding packets for each other to let them to communicate outside the range of direct wireless transmission or with each other. Ad Hoc networks do not have centralized administration or fixed network infrastructure such as base stations or access points, and can be speedily and economically deployed as required [1]. Due to mobility of nodes, the network topology of ad-hoc network may vary dynamically time to time. The network is distributed, so all the network activities like finding routes from source to destination, topology discovery and packet transmission must be executed by the mobile nodes. Therefore, routing functionality for packet transmission must be built-in. Examples of wireless nodes are personal computers (desktops/laptops) with wireless LAN cards, Personal Digital Assistants (PDA), or other types of wireless or mobile communication devices [2]. Figure 1 shows an overview of MANET. A wireless node can be any computing device that uses the air as a transmission medium. As shown in figure 1, to allow wireless communication among a person, a vehicle, or an airplane the wireless node may be physically attached to them. A wireless node can act like a source (initial point from where sending the data takes place), the destination (end point of data reception), or an intermediate node (routing of packets from source to destination) of data transmission. The network topology changes dynamically due to nodes tend to keep moving. Ad Hoc network have many advantages like Fast deployment, Low cost of deployment, Dynamic Configuration etc. Ad Hoc network is used in various purposes [3]. Few examples are emergency search and rescue operations, meeting events or conferences, and battlefield communication between moving vehicles and soldiers. With the abilities to meet the new demand of mobile computation, the MANET has a very bright future. In MANET, all the nodes work together to forward the packets in the network, and hence each and every node is working as a router. Thus one of the most important issues is routing in ad-hoc network. Some of the other issues in ad hoc networks are Distributed network, Dynamic topology, Power awareness, Addressing scheme, Network size and Security [4].

1.2 Characteristics of an Ideal Routing Protocol for Ad Hoc Wireless Network
Due to the issues in ad hoc wireless network environment discussed so far, wired network routing protocols cannot be used in ad-hoc wireless networks. Hence ad hoc wireless networks require specialized routing protocols that can deal with the challenges discussed above. A routing protocol for ad hoc wireless networks should be fully distributed, adaptable to frequent topology changes, route computation and maintenance involves minimum number of nodes, minimum connection set up time, localized, loop- free, minimum packet collisions and free from stale routes.

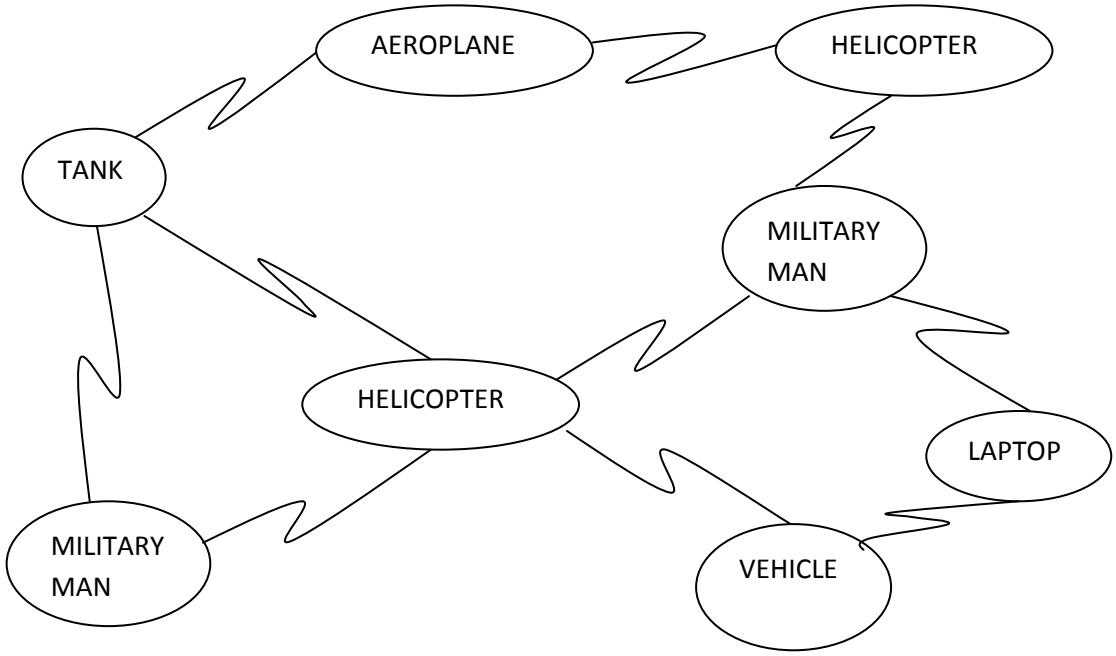
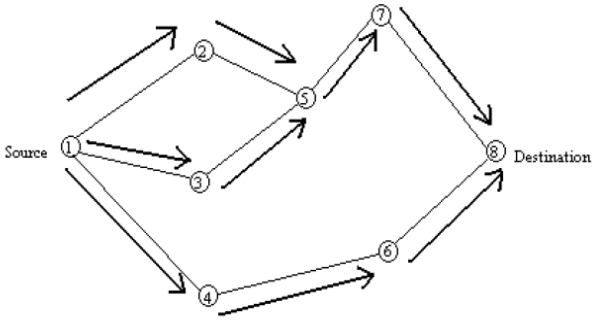


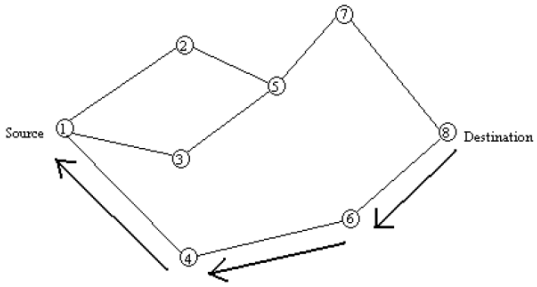
Fig 1: Overview of Mobile Ad-hoc Network

1.3 Dynamic Source Routing (DSR)

Dynamic Source Routing (DSR) is a routing protocol for wireless ad-hoc networks. It creates a route on-demand when a transmitting mobile node also known source node requests for the route. However, it uses source routing instead of depending upon the routing table at each intermediate device [5].Dynamic source routing protocol (DSR) is an on-demand, source routing protocol, where all the routing information is available at mobile nodes. DSR permits the network to be fully self-organizing and self-configuring, without the need for any pre-existing network administration. DSR is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain routes to random or unknown destinations in the ad- hoc network [6]. A best possible path for communication between a source node and destination node is decided by Route Discovery process. Route Maintenance make sure that the communication path remains best possible or most favorable and loop free according to the change in network conditions, even if this requires changing the route during a transmission. Route Reply would only be generated if the message has reached the decided destination node. To send the Route Reply, the destination node must have a route or path to the source node. If the route is in the route cache of destination node, the route would be used. Otherwise, the node will reverse the route based on the route record in the Route Reply message header. In the event of failure, the Route Maintenance Phase is started whereby the Route Error packets are generated at a node. The incorrect hop will be removed from the node's route cache; all routes containing the hop are reduced at that point. Again, the Route Discovery Phase is initiated to determine the most optimum route. The major difference between dynamic source routing and the other on-demand routing protocols is that it is beacon-less (broadcasting hello packets to its neighbours) and hence it does not have need of periodic hello packet (beacon) transmissions, which are used by a node to inform its neighbours of its presence. The fundamental approach of this protocol during the route creation phase is to launch a route by flooding Route Request packets in the network. When destination node receives a Route Request packet, it transfers a Route Reply packet to the source, which contains the route navigated by the Route Request packet received.



(a). Propagation of route request (RREQ) packet



(b). Path taken by the Route Reply (RREP) packet

Fig 2: Creation of route in DSR

A destination or target node, after receiving the first Route Request packet, replies to the source node via reverse path that the Route Request packet had traversed. Nodes can also be skilled about the neighboring routes traversed by data packets if operated in the immoral mode. This route cache is also used during the route construction phase. If an intermediate node receiving a Route Request has a route to the destination node in its route cache, then it replies to the source node by sending a Route Reply with the complete route information from the source node to the destination node [7].

1.3.1 Advantages and Disadvantages: DSR uses a reactive or on-demand approach which eliminates the need to periodically (from time to time) flood the network with table update messages which are required in a table driven approach. The intermediate nodes also make use of the route cache information proficiently to reduce the control overhead [7]. The disadvantage of DSR is that the route maintenance mechanism does not repair a broken down link in the neighbourhood. The connection setup holdup time is higher than in table driven protocols. Even though the protocol performs well in static and low-mobility environments, the performance degrades quickly with increasing mobility. The routing overhead is also involved due to the source-routing mechanism is used. This routing overhead is directly proportional to the path length i.e. if the route length increase overhead will also increase [8].

1.4 Black Hole Attack

A node announces a zero metric for all destinations causing all nodes around it to route data packets towards it. The AODV protocol is weak to such an attack. This type of attack is described in detail in [9]. In a black hole attack, a malicious or attacker node sends fake routing information to all the nodes in network, declaring that it has a best possible route and causes other good nodes to route data packets through the attacker node. For example, in DSR, the attacker can send a fake RREP to the source node. Fake RREP includes a fake destination sequence number that is made-up to be equal or higher than the one contained in the RREQ, declaring that it has a suitably fresh route to the destination node. This causes the source node to select the route that passes through the malicious node. Therefore, all traffic will be routed through the malicious node, and therefore, the malicious node can misuse or discard the traffic. As for gray hole, its behaviour is similar to a black hole. 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 a malicious node [10]. 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%.

2. METHODOLOGY

Figure 3 has showed the algorithm of finding route from source to destination by avoiding blackhole node based on faith values.

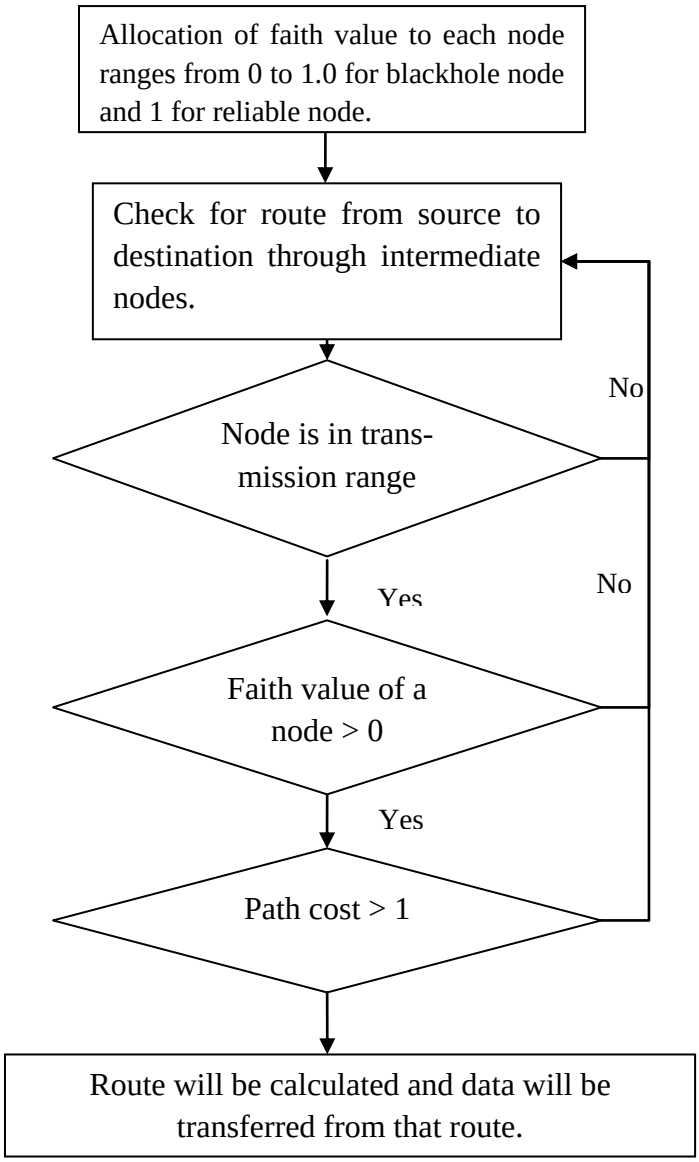


Fig 3: Algorithm of proposed technique

3. RESULTS AND ANALYSIS

The simulation was carried out in MATLAB R2008a. Simulation parameters are shown in table 1. We have 20 nodes for simulation and traffic type is random waypoint, where percentage of malicious node is 5% i.e. one node will act as blackhole in this simulation. The area for simulation is 100 m X 100 m.

The assumptions are node 1 will act as source and node 20 will act as destination, whereas node 19 will act as blackhole.

Table 1: Input Parameters for Simulation

Parameter	Value
Number of Nodes	20
Terrain dimension	100 m x 100 m
Traffic Type	Random waypoint
Simulation	200

Rounds	
% of malicious Nodes	10% of total nodes
MAC protocol	IEEE 802.11

Figure 4 have showed the process of route selection in DSR routing protocol.

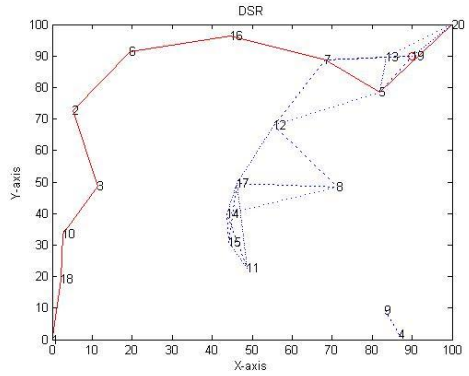


Fig 4: DSR route selection process

Figure 5 have showed the Route selection through blackhole node. In this process data is followed by balckhole which can create an error.

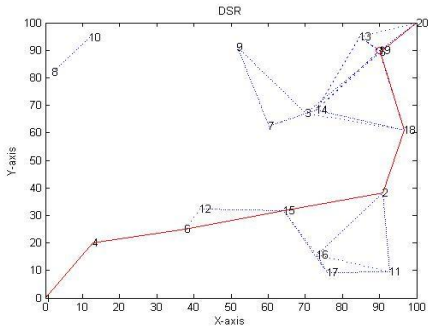


Fig 5: DSR route selection through blackhole node

Figure 6 and figure 7 have showed the route selection process of Secure-DSR by avoiding blackhole node from route selection process.

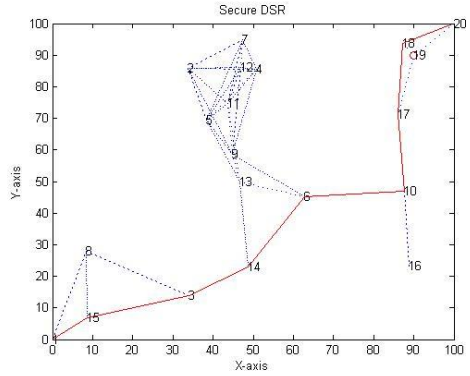


Fig 6: FaithDSR route selection process

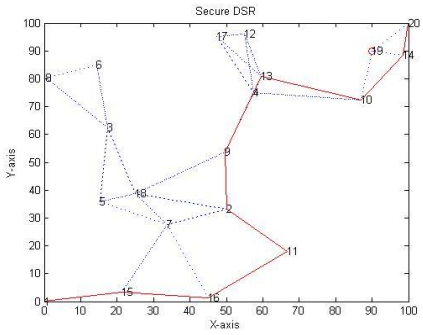


Fig 7: FaithDSR route selection process

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. In this total 200 packets are sent, DSR sent all packets with interception while there is no interception in secure DSR

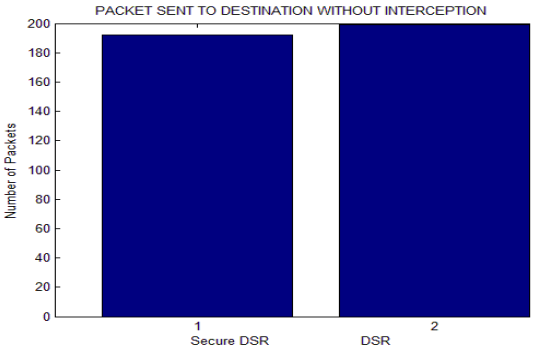


Fig 8: Packet sent to destination without interception though black hole

Figure 9 have showed the comparison between Secure-DSR and DSR routing technique in terms of packet sent to destination with interception through black hole.

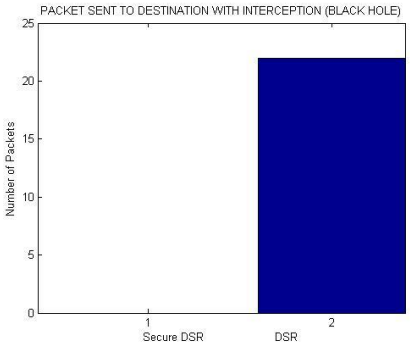


Fig 9: Packet sent to destination with interception through black hole

Figure 10 have showed comparison of both techniques in terms of finding route from source to destination. Faith DSR takes less time in finding routes as compared to DSR.

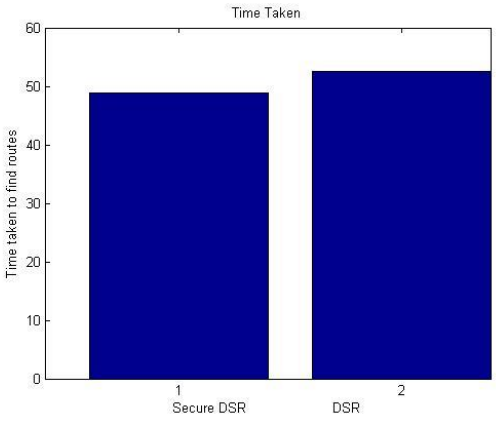


Fig 10: Total time taken to find route from source to destination

4. CONCLUSION AND FUTURE WORK

In this work, 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 Faith-DSR will avoid routing of packets through black hole nodes. After introducing and analyzing the concept of node-based trust in MANET, for future research we suggest to develop trust management schemes with desirable attributes such as adaptation to environmental dynamics, scalability and reliability.

5. REFERENCES

[1] P Narayan, V R. Syrotiuk,"Evaluation of the AODV and DSR Routing Protocols Using the MERIT Tool", In 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 Mobile Networks*, Vancouver, British Columbia, Canada, 27-28 Oct. 2008, pp. 83-90.

[7] 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.

[8] 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.

[9] 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.

[10] 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.