International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Secure Dynamic Source Routing Using Node's Faith Value in Mobile Ad-Hoc Network

Prerna Kaushik[1], Puneet Sharma[2]
[1]M.Tech student, [2]Assistant Professor
[1,2]Department of Computer Science and Engineering
Hindu college of Engineering, Sonipat, HARYANA-131001

Abstract: ***A mobile ad-hoc network is an autonomous group of mobile users that communicate over reasonably slow wireless links. The network topology may vary rapidly over time, because the nodes are mobile. The network is decentralized, where all network activity, including discovering the topology and delivering messages must be executed by the nodes themselves. 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. 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.***

Keywords: Secure routing, MANET, DSR, Faith DSR

I. INTRODUCTION

Mobile Ad-hoc networks are self-organizing and self-configuring multihop wireless networks, where the structure of the network changes dynamically. This is mainly due to the mobility of the nodes [1]. Nodes in these networks utilize the same random access wireless channel, cooperating in an intimate manner to engaging themselves in multihop forwarding. The node in the network not only acts as hosts but also as routers that route data to/from other nodes in network [2]. In mobile ad-hoc networks there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transferring packets; so there is need of a routing procedure. This is always ready to find a path so as to forward the packets appropriately between the source and the destination. Within a cell, a base station can reach all mobile nodes without routing via broadcast in common wireless networks. In the case of ad-hoc networks, each node must be able to forward data for other nodes. This creates additional problems along with the problems of dynamic topology which is unpredictable connectivity changes [3].

A. Properties Of Ad-Hoc Routing protocols

The properties that are desirable in Ad-Hoc Routing protocols are [4]:

1) Distributed Operation: The protocol should be distributed. It should not be dependent on a centralized controlling node. This is the case even for stationary networks. The dissimilarity is that the nodes in an ad-hoc network can enter or leave the network very easily and because of mobility the network can be partitioned.

2) Loop Free: To improve the overall performance, the routing protocol should assurance that the routes supplied are loop free. This avoids any misuse of bandwidth or CPU consumption.

3) Demand Based Operation: To minimize the control overhead in the network and thus not misuse the network resources the protocol should be reactive. This means that the protocol should react only when needed and should not periodically broadcast control information.

4) Unidirectional Link Support: The radio environment can cause the formation of unidirectional links. Utilization of these links and not only the bi-directional links improves the routing protocol performance.

5) Security: The radio environment is especially vulnerable to impersonation attacks so to ensure the wanted behavior of the routing protocol we need some sort of security measures. Authentication and encryption is the way to go and problem here lies within distributing the keys among the nodes in the ad-hoc network.

6) Power Conservation: The nodes in the ad-hoc network can be laptops and thin clients such as PDA_s that are limited in battery

power and therefore uses some standby mode to save the power. It is therefore very important that the routing protocol has support for these sleep modes.

7) Multiple Routes: To reduce the number of reactions to topological changes and congestion multiple routes can be used. If one route becomes invalid, it is possible that another stored route could still be valid and thus saving the routing protocol from initiating another route discovery procedure.

8) Quality Of Service Support: Some sort of Quality of service is necessary to incorporate into the routing protocol. This helps to find what these networks will be used for. It could be for instance real time traffic support.

B. Applications Of MANET

Mobile ad hoc networks have been employed in scenarios where an infrastructure is unavailable, the cost to deploy a wired networking is not worth it, or there is no time to set up a fixed infrastructure. In all these cases, there is often a need for collaborative computing and communication among the mobile users who typically work firefighters facing a hazardous emergency, policemen conducting surveillance of suspects, and soldiers engaging in a fight. Another application area is communication and coordination in a battlefield using autonomous networking and computing [5,6]. Some military ad hoc network applications require unmanned, robotic components. Unmanned Airborne Vehicles (UAVs) can cooperate in maintaining a large ground mobile ad hoc network interconnected in spite of physical obstacles, propagation channel irregularities, and enemy jamming. The UAVs can help meet tight performance constraints on demand by proper positioning and antenna beaming. A vehicular ad hoc network (VANET) is a mobile ad hoc network designed to provide communications among close vehicles and between vehicles and nearby fixed equipment. The main goal of a VANET is to provide safety and comfort for passengers. To this end, a special electronic device is placed inside each vehicle that will provide ad hoc network connectivity for the passengers and vehicle. Generally, applications in a VANET fall into two categories, namely safety applications and comfort applications [6]. Safety applications aim to provide driver's information about future critical situations and, hence, have strict requirements on communication reliability and delay. Some of the safety applications envisioned for VANETs are inter-vehicle danger warning, intersection collision avoidance, and work zone safety warning. With numerous emerging applications, opportunistic ad hoc networks have the potential to allow a large number of devices to communicate end-to-end without requiring any pre-existing infrastructure and are very suitable to support pervasive networking scenarios.

C. Advantages and Limitations Of MANET

The advantages of MANET are [9]:

Router Free
Mobility
Speed
Fault Tolerance
Connectivity
Fast Installation
Economical

The limitations of MANET are [10]:

Bandwidth Constraints
Processing capability
Energy constraints
High Latency
Transmission Errors
Security
Location
Roaming
Commercially Unavailable

II. DSR PROTOCOL

The DSR Protocol is a simple and efficient routing protocol designed specifically for use in multihop wireless ad hoc networks of mobile nodes. Using DSR, the network is completely self-organizing and self-configuring, requiring no existing network infrastructure or administration. Network nodes (computers) cooperate to forward packets for each other to allow communication over multiple "hops" between nodes not directly within wireless transmission range of one another [7]. As nodes in the network move about or join or leave the network, and as wireless transmission conditions such as sources of interference change, all routing is automatically determined and maintained by the DSR Routing Protocol. Because the number or sequence of intermediate hops needed to reach any destination may change at any time, the resulting network topology may be quite rich and rapidly changing. The DSR Protocol allows nodes to dynamically discover a source route across multiple network hops to any destination in the ad hoc network. While designing DSR, we needed to create a routing protocol that had very low overhead yet was able to react quickly to changes in the network, providing highly reactive service to help ensure successful delivery of data packets in spite of node movement or other changes in network conditions.

A. Overview And Important Properties Of The Protocol

The DSR Protocol is composed of two mechanisms that work together to allow the
discovery and maintenance of source routes in the ad hoc network:
Route discovery is the mechanism by which a node S wishing to send a packet to a destination node D obtains a source route to D. Route discovery is used only when S attempts to send a packet to D and does not already know a route to D.
Route maintenance is the mechanism by which node S is able to detect, while using a source route to D, if the network topology has changed such that it can no longer use its route to D because a link along the route no longer works. The DSR Protocol is a simple and efficient routing protocol designed specifically for use in multihop wireless ad hoc networks of mobile nodes. Using DSR, the network is completely self-organizing and self-configuring, requiring no existing network infrastructure or administration. Network nodes (computers) cooperate to forward packets for each other to allow communication over multiple "hops" between nodes not directly within wireless transmission range of one another. As nodes in the network move about or join or leave the network, and as wireless transmission conditions such as sources of interference change, all routing is automatically determined and maintained by the DSR Routing Protocol. Because the number or sequence of intermediate hops needed to reach any destination may change at any time, the resulting network topology may be quite rich and rapidly changing. The DSR Protocol allows nodes to dynamically discover a source route across multiple network hops to any destination in the ad hoc network. Each data packet sent then carries in its header the complete, ordered list of nodes through which the packet must pass, allowing packet routing to be trivially loop-free and avoiding the need for up-to-date routing information in the intermediate nodes through which the packet is forwarded. By including this source route in the header of each data packet, other nodes forwarding or overhearing any of these packets may also easily cache this routing information for future use. While designing DSR, we needed to create a routing protocol that had very low overhead yet was able to react quickly to changes in the network, providing highly reactive service to help ensure successful delivery of data packets in spite of node movement or other changes in network conditions.

III. 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 [8]. Fig. 1 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.

Volume 3 Issue IX, September 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

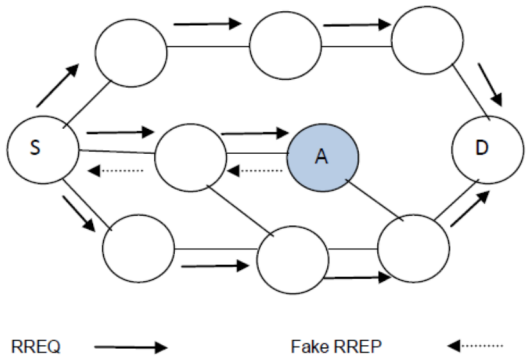

Figure 1. Example of a Black Hole Attack on DSR.

IV. PROPOSED METHODOLOGY

Here we are proposing a secure routing technique to deliver the data packets from source to destination.
In this technique, we have added nodes faith values according to its cooperation in delivering data packets.
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.
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.
We have applied dijkstra algorithm to find out the shortest route or path from source to destination.
We have supplied three input parameters to dijkstra algorithm. Source node, Destination node and nodes faith values.
We can calculate shortest path based on faith values and total distance or cost by using Dijkstra algorithm .

V. IMPLEMENTATION & RESULTS

The simulation was carried out in MATLAB R2013. Simulation parameters are shown in table 1. We have 10 nodes for simulation and traffic type is random waypoint, where percentage of malicious node is 10% i.e. one node will act as blackhole in this simulation. The area for simulation is 50 m X 50 m. In this work, Node 1 will act as source node from where packet will initiate and node 10 will act as destination, whereas node 9 will act as blackhole.

Table 1: Simulation Parameters

Number of Nodes	10
Terrain dimension	50 m x50 m
Traffic Type	Random waypoint
Simulation Rounds	100
% of malicious nodes	10% of total nodes
MAC protocol	IEEE 802.11

Figure 2 have showed the process of route selection in DSR routing protocol. Route selection through blackhole node is shown in figure 3. Figure 4 and figure 5 have showed the route selection process of Secure-DSR by avoiding blackhole node from route selection process. Figure 6 have showed the comparison between Secure-DSR and DSR routing technique in terms of packet sent to destination without interception though black hole. Figure 7 have showed the comparison between Secure-DSR and DSR routing technique in terms of packet sent to destination with interception through blackhole.

Volume 3 Issue IX, September 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

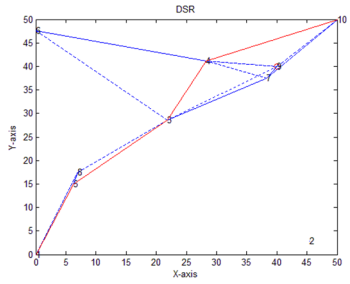

Figure 2: DSR route selection process

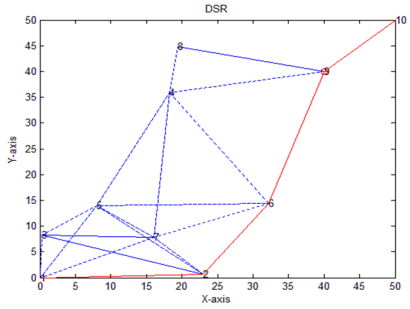

Figure 3: DSR route selection through blackhole node

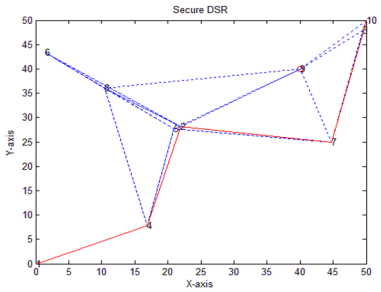

Figure 4: Secure DSR route selection process

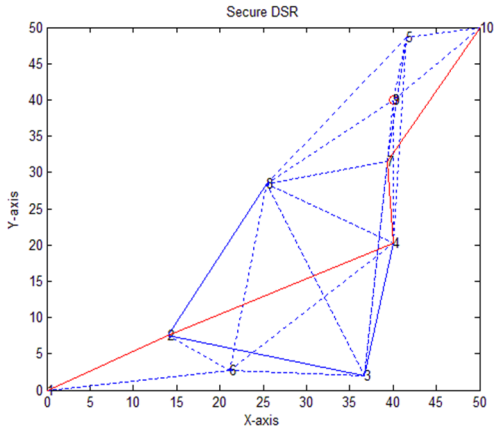

Figure 5: Secure DSR route selection process

Volume 3 Issue IX, September 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

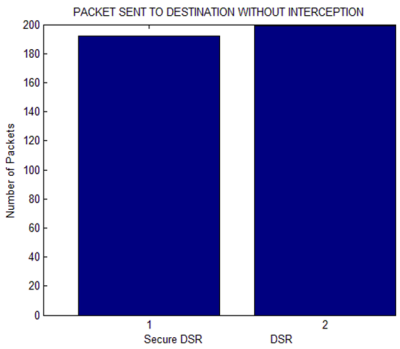

Figure 6: Packet sent to destination without interception though black hole

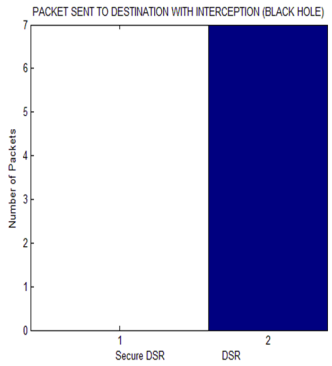

Figure 7: Packet sent to destination with interception through black hole

VI. 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 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.