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

A Review of Secure Routing Techniques in Mobile Ad-hoc Network

Prerna Kaushik[1], Puneet Sharma [2]

[1]M.Tech student
Department of Computer Science and Engineering
Hindu college of Engineering,Sonipat,HARYANA-131001
prernakaushik10@gmail.com

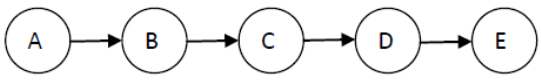
[2]Assistant Professor
Department of Computer Science and Engineering,
Hindu college of Engineering,Sonipat,HARYANA-131001
puneet.hce@gmail.com

***Abstract**: A mobile ad-hoc network (MANET) is a collection of wireless mobile nodes organized to create a short-term connection between them. Nodes communicate with each other through single-hop or multi-hops. Each mobile node has a limited transmission range. Nodes in mobile Ad Hoc Network (MANET) do not depend on a central infrastructure but transmit packets originated by other mobile nodes. Due to lack of centralized control, the condition of making routing secure in mobile ad hoc networks is much more challenging than the security in wired network or infrastructure based networks. Mobile ad hoc networks can work properly only if the participating nodes cooperate in routing and forwarding. In this paper, we propose a new approach in dynamic source routing (DSR) protocol 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 proposed algorithm will be helpful in avoiding black hole node.*

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.



1. A----->B : (A) ID=2
2. B---- > C: (A, B) ID=2
3. C---->D :(A, B, C) ID=2
4. D----> E :(A, B, C, D) ID=2

Fig.1: Route Discovery process

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

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

[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*. 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. 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. 2, 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. 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.

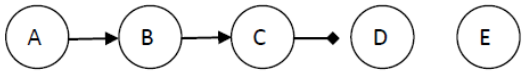


Fig. 2: Route Maintenance Process

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.

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

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

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. 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.

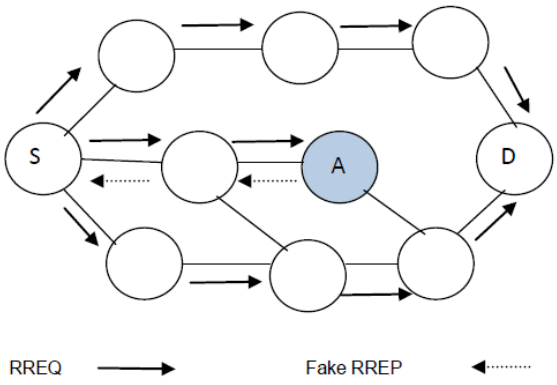


Fig. 3: Example of a Black Hole Attack on DSR.

2. RELATED WORK

Several works propose monitoring schemes to generate trust values describing the trustworthiness, reliability, or competence of individual nodes. Secure routing is an important issue in MANETs. A particularly devastating attack in wireless networks is the black hole attack. The performance of ad hoc networks depends on cooperation and trust among distributed nodes. To enhance security in ad hoc networks, it is important to evaluate trustworthiness of other nodes without centralized authorities. As a result, an efficient algorithm to detect black hole attack is important. In this paper [1], to improve the quality a modified design of trust based dynamic source routing protocol is proposed. Each node would evaluate its own trusted parameters about neighbors through evaluation of experience, knowledge and recommendations. This protocol discovers multiple loop-free paths which are evaluated by hop count and trust. This judgment provides a flexible and feasible approach to choose a shortest path in all trusted path. The proposed protocol reduces the packet loss due to malicious nodes to a considerable extent thereby enhancing the performance. The author also compares the simulation results of with and without the proposed secure trust based model. The simulation results demonstrate that the PDR for STBDSR falls from 92% to 80%.A mobile ad-hoc network is a self-configuring network of mobile hosts connected by wireless links which together form an arbitrary topology. Due to lack of centralized control, dynamic network topology and multihop communications, the provision of making routing secure in mobile ad hoc networks is much more challenging than the security in infrastructure based networks. But due to their limitations, there is a need to make them robust and more secure so that they can go well with the demanding requirements of ad hoc networks. This paper [2] presents a survey of trust based secure routing protocols for mobile ad hoc networks. Different trust based secure routing protocols are discussed and analyzed in the paper along with their strengths, weaknesses and future enhancements. The odorakopoulos and Baras [5] analyze the issue of evaluating the trust level as a generalization of the shortest-path problem in an oriented graph, where the edges correspond to the opinion that a node has about other node. They consider that nodes use just their own information to establish their opinions. The opinion of each node includes the trust level and its precision. The main goal is to enable nodes to indirectly build trust relationships using exclusively monitored information. Moe *et al.* [6] proposed a trust-based routing protocol as an extension of DSR based on an incentive mechanism that enforces cooperation among nodes and reduces the benefits that selfish nodes can enjoy (e.g., saving resources by selectively dropping packets). This work is unique in that they used a hidden Markov model (HMM) to quantitatively measure the trustworthiness of nodes. In this work, selfish nodes are benign and selectively drop packets. Performance characteristics of the protocol when malicious nodes perform active attacks such as packet modifications, identity attacks, etc., need to be investigated further. Sun *et al.* [7] proposed trust modeling and evaluation methods for secure ad hoc routing and malicious node detection. The unique part of their design is to consider trust as a measure of uncertainty that can be calculated using *entropy*. In their definition, trust is a continuous

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

variable, and does not need to be transitive, thus capturing some of the characteristics of trust in MANETs. However, this work considers packet dropping as the only component of direct observations to evaluate trust. Balakrishnnan *et al.* [8] developed a trust model to strengthen the security of MANETs and to deal with the issues associated with recommendations. Their model utilizes only trusted routes for communication, and isolates malicious nodes based on the evidence obtained from direct interactions and recommendations. Their protocol is described as robust to the recommender's bias, honest-elicitation, and free-riding. This work uniquely considered a context-dependency characteristic of trust in extending DSR. A Combiner computes the final trust in a node based upon the information it receives from the Trust and Reputation agents. Trust is computed using direct and indirect information. The trust value is propagated by piggybacking the direct trust value of the nodes along with RREQ packets [9]. The Trust-embedded AODV (T-AODV) routing protocol [10] was designed to secure an ad hoc network from independent malicious nodes by finding a secure end-to-end route. In this protocol, trust values are distributed to the nodes a priori. In the route discovery phase the RREQ packet header contains a trust level field, in addition to the other fields. In [11], the authors have designed a secure routing protocol, called Trust based multi path DSR protocol, which depends on two-way effort of the node by embedding trust to find an end-to end secure route free of misbehaving nodes. This protocol has a drawback routing overhead is very high compared to traditional DSR due to broadcasting of RREQ packet.

3. PROPOSED METHODOLOGY

1. In this work, 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 .

For calculation of faith values between two nodes. The equation is

faith(i,j)=((Z(i)+Z(j))/2) (1) where Z(i) is the faith value of i^{th} node and Z(j) is the faith value of j^{th} node.

4. CONCLUSION

Security is an important issue in mobile ad-hoc network. Various algorithms have been proposed till now to secure the routing in mobile ad-hoc network, but there is still need for improvement. In this paper, we propose a new approach in dynamic source routing (DSR) protocol 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 proposed algorithm will be helpful in avoiding black hole node; therefore it will eliminate black hole attack.

REFERENCES

[1] Poonam, K. Garg, M. Misra, "Trust Enhanced Secure Multi-Path DSR Routing" ***International Journal of Computer Applications (0975 – 8887) Volume 2 – No.2, May 2010* .**

[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,*** **2010, pp. 1-22.**

[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.**

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

[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] Sivakumar, K.A.; Ramkumar, M., "An Efficient Secure Route Discovery Protocol for DSR," *Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE* , vol., no., pp.458,463, 26-30 Nov. 2007

[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] Pirzada, A. A., Datta, A. and McDonald, C. 2004. Trustbased routing for ad-hoc wireless networks. In Proceeding of. IEEE International Conference Networks (Singapore, 2004). 326-330.

[10] Pissinou, N., Ghosh, T. and Makki, K. 2004. Collaborative trust-based secure routing in multihop ad hoc networks. Networking (Athens, Greece 2004). Lecture Notes in Computer Science, vol. 3042, 1446-1451.

[11] Poonam, Garg, K., and Misra, M. 2010. Trust based multi path DSR protocol. In Proceedings of Fifth International Conference on Availability, Reliability and Security,(Poland, February, 2010). 204-209.