IMPROVING ENERGY EFFICIENCY & SECURITY IN DSR ROUTING PROTOCOL

Poonam Mishra[1], Neelesh Gupta[2]

M.Tech Scholar, HOD (EC Dptt.),

Truba Institute of Engineering & Information Technology, Bhopal (India)

ABSTRACT

Mobile Ad-Hoc Networks (MANETs) are wireless networks consisting of a collection of nodes having no fixed infrastructure. The nodes use typically autonomous sources of energy that have a limited battery lifetime. Therefore, reducing energy consumption is an important design criterion for routing protocols in mobile ad-hoc networks. Also, mobile ad-hoc networks are more prone to suffer from the malicious behaviors than the traditional wired networks. Therefore, it also becomes very much necessary to pay attention to the security issues in the mobile ad-hoc networks. In this paper these two issues of energy efficiency and security are carried out simultaneously by using DSR routing protocol. DSR has two mechanisms of "Route Discovery" and "Route Maintenance". During "Route Maintenance" the path breakage occurs due to the less battery power of the nodes. In this work, the nodes with very less energy are dynamically replaced by the nodes having sufficient amount of energy. And at the same time a 2ACK scheme is proposed that detects the malicious behavior of nodes to maintain security in DSR routing protocol. These two methods are used simultaneously to make secure and efficient routing in MANET at same time.

Keywords: MANET, DSR, MDSR, 2ACK scheme, RREQ, RREP, LRREQ

I. INTRODUCTION

Mobile Ad-Hoc Networks (MANETs) [1] are wireless networks consisting of a collection of untethered nodes with no fixed infrastructure. Nodes in a MANET participate in forwarding data packets when the two end-points are not directly within their radio range. The MANETs present characteristics such as dynamic topologies, bandwidth-constrained, variable-capacity links, and energy-constrained operations that will affect protocol design [2]. Routing protocols design for MANETs is a very active research area and many proactive and reactive protocols have been proposed [3]. Proactive protocols find routes between all source-destination pairs regardless of the actual need for such routes. The more traditional proactive protocol can reduce the needed time to get a route by inducing a high routing load over the network. Reactive protocols, on the other hand, are based on the reduction of the routing load by initiating new routing. The challenge for MANET routing protocols is to provide a communication platform that is solid, adaptive and dynamic in the face of widely fluctuating wireless channel characteristics and node mobility. Nodes in MANET may move freely and randomly. Therefore, the network topology of a MANET can be change unpredictably and speedily. As these nodes have the flexibility of moving from one place to other, there may be cases wherein a particular node which is a receiver for a particular packet, moves away from the range of sender. However, the sender is not aware of this scenario and it might still keep on sending packets thus leading to packet and data loss. A malicious node drops packets or generates additional packets solely to disrupt the network performance and prevent other nodes from accessing any network services (a denial of service attack). Misbehavior can be divided into two categories: routing misbehavior (failure to behave in accordance with a routing protocol) and packet forwarding misbehavior (failure to correctly forward data packets in accordance with a data transfer protocol. However, a node may misbehave by agreeing to forward packets and then failing to do so, because it is overloaded, selfish, malicious, or broken. A selfish node is unwilling to spend battery life, CPU cycles, or available network bandwidth to forward packets not of direct interest to it, even though it expects others to forward packets on its behalf. A malicious node launches a denial of service attack by dropping packets. A broken node might have a software fault that prevents it from forwarding packets [4]. Misbehaving nodes can be a significant problem. On the other hand the resources present in MANET are limited, e.g., battery power. It is very important resource as it has limited life and is not easily rechargeable. So we have to reduce the energy consumption in MANET by using an efficient routing algorithm for data transmission. In this paper an energy efficient method has been proposed which causes dynamic change of routes when any chance of path breakage occurs by considering the node mobility and battery power simultaneously that helps in saving the network energy. And also a scheme is used to secure the network from the misbehaving of nodes. The work is carried out on DSR routing protocol.

II. DSR ROUTING SCHEME

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad-hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol 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 arbitrary destinations in the ad hoc network.

2.1 Route Discovery

The route discovery comes in play when a mobile node has some data/packet to send to any destination and it does not have any route to the destination in its route cache [5]. Then it initiates route discovery by broadcasting a route request (RREQ) packet. This route request contains address of the destination, address of the source and a unique identification number that is generated by the source node only. Each node receives the packet and checks whether the packet is meant for it or not. If it is not the destination node then it simply forwards the packet to the outgoing links adding its own address in the packet. To avoid duplicate route request which is generated from the same source, a node only forwards the route request that has not yet been seen appear in the route request with the same identification number. As soon as the packet arrives at the destination node or arrives at a node that contains in its route cache an unexpired route to the destination, then a route reply is generated. Not only the packet contains all the address of the intermediate node it has come across but the sequences of hops are also stored in it. The Route reply (RREP) is generated by the destination placing the route record contained in the route request into route reply. During the route reply if the destination node has the route to the initiator in its route cache, it may use that route for route reply. Otherwise destination node may reverse the route in the route record if the link is symmetric. If the symmetric links are not supported then the node may initiate its own route discovery piggybacking the route reply on the new route request. When any intermediate node receives any route reply from destination node or any other node then they append their route record and forward it to its neighbor nodes.

2.2 Route Maintenance

In DSR every node is responsible for confirming that the next hop in the source route receives the packet [8]. Also each packet is only forwarded once by a node (hop-by-hop routing). If a packet can't be received by a node, it is retransmitted up to some maximum number of times until a confirmation is received from the next hop. Only if retransmission results then in a failure, a Route Error message is sent to the initiator that can remove that source route from its Route Cache. So the initiator can check his Route Cache for another route to the target. If there is no route in the cache, a Route Request packet is broadcasted.

III. RELATED WORK

An important design criterion for routing protocols in ad hoc networks is power consumption reduction. In this paper [10] an energy-efficient mechanism is described that can be used by a generic MANET routing protocol to prevent nodes from a sharp drop of battery power. This mechanism is applied to the Dynamic Source Routing (DSR) and proposes a novel DSR based energy efficient routing algorithm referred to as the Energy-Dependent DSR (EEDSR). The continuous evaluation of the energy budget of a node along an active route in EDDSR prevent nodes from being overwhelmed by network traffic, thereby contributing to better load balancing and a fair energy utilization. EDDSR shows a similar behavior that MDR, however EDDSR has the additional merit of being compatible with the use of the route cache used by DSR. The study proved that MDR and EDDSR clearly outperform DSR in terms of node lifetime especially in dynamic scenarios.

In Wireless communications the traffic across a mobile ad hoc network (MANET) can be highly vulnerable to security threats. The mobile ad hoc networks are more prone to suffer from the malicious behaviors than the traditional wired networks. Therefore, it becomes very much necessary to pay more attention to the security issues in the mobile ad hoc networks. The presence of malicious node will interrupt the packets and causes unwanted changes. In order to avoid these problems signature verification is done at every hop using new algorithm. This algorithm increases the amount of data received with respect to time and increases the throughput. To reduce this constrain in this paper [8] a new algorithm is proposed by using Dynamic Source Routing (DSR) protocol. In this algorithm malicious nodes are checked using signature verification in every node. If it finds any malicious nodes, the traffic will be rerouted through another path.

The nodes in the mobile ad hoc networks use typically autonomous sources of energy that have a limited battery lifetime. It is therefore important to minimize the energy consumption of nodes in the wireless networks. This paper [9] propose a new energy efficient algorithm for the dynamic source routing protocol (DSR) which is based on the network topology precisely the approach of enclosure graph and relay region in which communicating through the relay node is more energy efficient than direct communication. In this topology, the network is strongly connected if each node maintains connections with all the existing nodes in its closure. The proposed method investigates distance between the nodes which is proportional with a transmission power used by a node and with the idle listening energy consumption. Our proposition contributes to preserve energy of mobiles units and ensure their connectivity in the routing process.

A Mobile Ad Hoc Network (MANET) is a collection of mobile nodes (hosts) which communicate with each other via wireless links either directly or relying on other nodes such as routers. Due to the dynamic change in topology finding route is very difficult. Some nodes misbehave as they participate in route establishment phase but refuse to forward the data packets to conserve their own energy. For detecting routing misbehavior in MANETs lot of techniques are there such as watchdog, pathrater, TWOACK, SACK, End to End ACK scheme.

But due to the disadvantages of the above scheme a new scheme is proposed in this paper [6] called 2ACK and the routing protocol used is Optimized Link State Routing (OLSR). The 2ACK scheme identified misbehavior in routing by using a new acknowledgment packet, called 2ACK packet.

Battery power of the node (Energy of the node) is an important resource for the MANET. The Ad-hoc On demand Distance Vector Routing is most widely used protocol in MANET. AODV routing protocol creates the routes On-demand when any node has some data for the communication. In AODV routes break due to the node mobility and/or less battery power. In this paper [7] two algorithms are proposed to improve the energy consumption and security of MANET. The proposed algorithms utilize the dynamic route shortening and local route repair scheme to improve the reliable packet delivery and enhance the route maintenance if route breaks occur due to less remaining energy in the nodes. The proposed schemes can be incorporated into any Ad-hoc on demand routing protocol.

IV. PROPOSED METHODOLOGY

In this paper energy efficient and security methods are proposed which is applied on DSR routing protocol simultaneously. The main design objective is to increase the lifetime of nodes with low energy reserves and to provide security from nodes misbehavior.

4.1 Security Model

The process starts when a source node has data packets to be sent to the destination, it initiates a Route Request packet. This Route Request is flooded throughout the network. The destination node, on receiving a Route Request packet responds by sending a Route Reply packet back to the source, which carries the route traversed by a Route Request packet received. Now consider a two hop path of N1→N2→N3 in which N1 is the source node and N3 is the destination node. Each node consists of a client and a server, the server on receiving the data packets from same nodes client forward the data packets to the next hop on the path. When node N1 wants to send data packet to node N3, the client of node N1 forwards the data packet to the server of node N1 which then forwards the data packet to the client of node N2. At the same time node N1 starts a timer. The process remains continue till the data packet reaches to client of node N3. After receiving the message the node N3 sends an ACK packet to node N1. Node N2 has to forward the packet to node N1. On receiving the 2ACK packet the status of the timer is checked by node N1 which was started for the data packet sent to node N3. If node N1 receives the data packet from node N3 after expiry of the timer or the data packet is not received at all then it will report node N3 as a malicious node. In case of misbehavior server doesn’t forward the 2ACK packet to the next hop client. When node N1’s client does not receive a 2ACK packet, it increments the number of packets missing. At the end of the process a ratio of the total number of data packets for which the 2ACK packet is not received to the total number of data packets sent is calculated and the considered link is declared as misbehaving link. If the ACK packet is not received then the corresponding node attached to that link is declared as misbehaving node.

4.2 Energy Model

In this model the main objective is to reduce the energy consumption in the route maintenance case in DSR routing protocol. In DSR a route is established only when it is required. The intermediate nodes also utilize the route cache information efficiently to reduce the control overhead. In original DSR protocol the route maintenance mechanism does not locally repair a broken link. State route cache information could also result in inconsistencies during the route reconstruction phase. In this proposed model the route is created locally by using the neighboring nodes which have the highest energy. This increases the life of the node. Energy weights of nodes are maintained on the basis of their remaining energy. If any node has the energy more than 70% then it is assigned the highest energy weight as it has sufficient energy to take part in the routing process and it can take part for a longer time. And if it has energy less than 30% then it is assigned the lowest energy and is not able to take part in the routing process for a longer time. Thus, the routing process avoids such type of nodes and minimum energy weight 1 is assigned to such node 1 otherwise weight 2 or more is assigned according to their energy weights. When any route breakage occurs during the data transmission then the upstream node creates the route locally and sends the local route request message (LRREQ) to the entire neighboring nodes, then all the neighboring nodes send the route reply message with their energy weights and the upstream node selects the highest energy weight among them. After the creation of new route on the basis of the remaining energy power in the node, the chances of route breakage is reduced and the network becomes more energy efficient.

V. SIMULATION RESULTS

The performance of proposed methods is implemented on network simulator (NS-2) and the results are compared with original DSR protocol to check the performance. So by the result comparison it can be seen that now there is less energy consumption in the network and now modified DSR performs better than the original DSR. To reduce the misbehavior of nodes in the network the security mechanism is implemented reducing the malicious behavior of nodes in the network. It is evident from the results that the proposed methods are able to save energy of the nodes as well as able to find the malicious nodes in the network. The simulation parameters used to implement the proposed methods are given in Table 1.

Parameters	Values
Simulation Tool	NS-2.34
Power Range(Transmission Range)	250
Number of nodes	10, 20, 30, 40, 50
Number of communication pair	5, 10
Topology size	600*600m^2
Mobility model	Random Way-point
Mobile Speed	10m/s
Routing Policy	DSR
Traffic type	CBR: constant bit rate
Packet Rate	20packets/sec
Packet size	512 bytes
Path loss model	Two-ray Ground
Mac Protocol	802.11 DCF
Interface queue type	CMUPriQueue
Simulation Time	120

The following parameters have been used for evaluation of the performance of proposed methods by varying number of nodes from 10, 20, 30, 40, and 50.

5.1 Packet Delivery Ratio (PDR)

It is the ratio of the total number of data packets received by the destination node to the total number of data packets sent.

5.2 Average End to End Delay

Average end-to-end delay is the delay experienced by the successfully delivered packets in reaching their destinations. It is the average of the delay difference of received time and sent time of every data packet.

5.3 Throughput

It is the ratio of the total amount of data that reaches a receiver from a sender to the time it takes for the receiver to get the last packet.

5.4 Energy Consumption

Battery power of a node is a precious resource that must be used efficiently in order to avoid early termination of a node or a network.

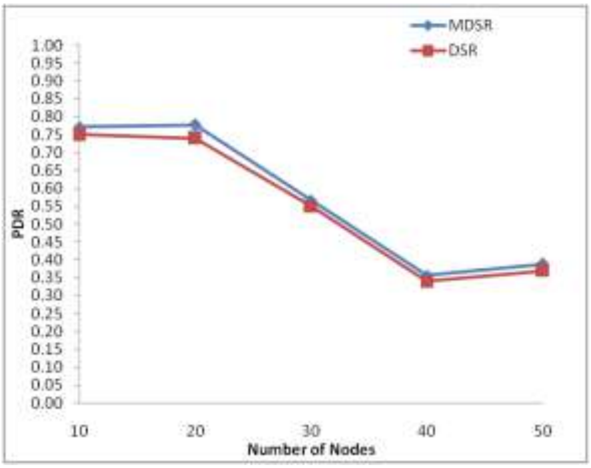

Fig 1 Packet Delivery Ratio Comparison by Varying Number of Nodes

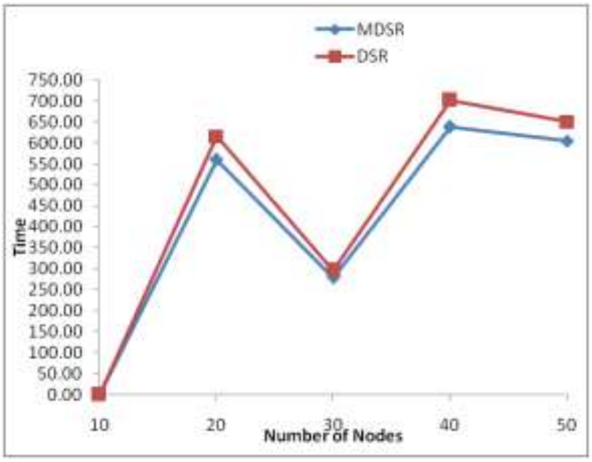

Fig 2 Average End to end Delay Comparison by Varying Number of Nodes

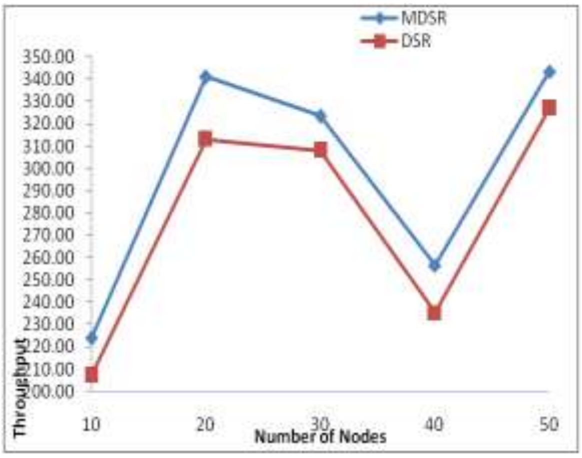

Fig 3 Throughput Comparison by Varying Number of Nodes

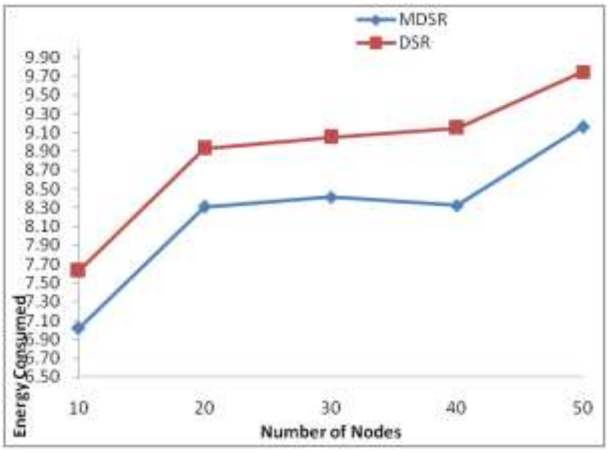

Fig 4 Comparison of the Energy Consumption for Varying Number of Nodes

The Packet Delivery Ratio (PDR) in the proposed method has been compared between the original DSR and modified DSR (MDSR) and is clearly seen from Fig1 that the proposed method is producing higher PDR for MDSR in comparison to the original DSR. Similarly, it is seen from the Fig2 that average end to end delay minimizes in proposed algorithm in comparison to original DSR. MDSR has the shortest end-to-end delay than DSR. It can also be seen from Fig3 that the proposed method gives better throughput for MDSR as compared to DSR. The increase in number of nodes in the network increases the energy consumption. In this case the proposed algorithm again works better than the DSR protocol. It is shown in Fig4 that MDSR consumes less energy than DSR.

V. CONCLUSION

In this paper, two methods are proposed to improve the energy consumption and security of MANET. The proposed algorithms enhance the route maintenance if route breaks occur due to less remaining energy in the nodes as well as detects routing misbehavior in the network. In the energy implementation part the dynamic route change strategy in the network is applied that tries to recover the route locally whenever any route breakage occurs because of less remaining energy in the node. While in security implementation part, the 2ACK technique is used to decrease the packet loss which helps to detect misbehavior of nodes by a 2 hop acknowledgment. The results indicate that MDSR is able to improve the energy efficiency and security in the network, discover the required path with less route breakage, the packet delivery ratio improved, the throughput is increased and the packet experienced a low average delay, consumes lesser time and is more reliable. This methodology is incorporated with the existing DSR protocol and the results shown that proposed scheme performs very well.

REFRENCES

[1] Internet Engineering Task Force, “Manet working group charter,” http://www.ietf.org/html.charters/manet-charter.html.

[2] S. Corson and J. Macker, “Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations,” RFC 2501, January 1999.

[3] E.Royer and C.-K. Toh, “A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks,” IEEE Personal Communications Magazine, Vol. 6, No. 2, April 1999.

[4] Baker M, Giuli T., Lai K. and Marti S, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks“, Proc. MobiCom, pp. 255-265, Aug. 2000.

[5] Baisakh, “A Review of Energy Efficient Dynamic Source Routing Protocol for Mobile Ad Hoc Networks” International Journal of Computer Applications (0975 – 8887) Volume 68– No.20, April 2013

[6] Prof. Shalini V. Wankhade, “2ACK-Scheme: Routing Misbehavior Detection in MANETs Using OLSR”, International Journal of Science, Engineering and Technology Research (IJSETR) Volume 1, Issue 1, July 2012.

[7] K. V. Arya, Senior Member, IEEE, and Kuldeep Narayan Tripathi, “Power Aware and Secure Routing in Mobile and Ad-Hoc Networks” 2013 IEEE 8th International Conference on Industrial and Information Systems, ICIIS 2013”, Aug. 2013, Sri Lanka.

[8] Sivasakthi. S, Seramannan. S, S. Rajesh, S.Thamilselvan, N. Premkumar, “MANETs Using Advance DSR Algorithm and Improve the Secure Transmission” International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 7, July 2013.

[9] Ahlem Drif, Abdellah Boukerram, “Energy Efficient DSR Algorithm based on Topology for Mobile Ad-Hoc Network” International Journal of Computer Applications (0975 8887) Volume 83 - No. 11, December 2013.

[10] J.-E. Garcia, A. Kallel, K. Kyamakya, K. Jobmann, J.-C. Cano, P. Manzoni, “A Novel DSR-based Energy-efficient Routing Algorithm for Mobile Ad-hoc Networks”.