# SECURE ROUTING PROTOCOL IN MANET BASED ON FITNESS OF A NODE


| Procheta Sen | Ritu Jain | Debasmita Dutta | Gairika Nandi |
|---|---|---|---|
| Student of IEM | Student of IEM | Student of IEM | Student Of IEM |
| Kolkata-700004 | Beldanga-742133 | Kolkata-700064 | Kolkata-700024 |
| (+91)9476143559 | (+91)9232778277 | (+91)8100862639 | (+91)9874771912 |
| ps208411@gmail.com | ritujain1009@gmail.com | debasmitadutta2009@gmail.com | gairika.09@gmail.com |



## ABSTRACT

Mobile Adhoc Networks(MANET) is a collection of mobile nodes that communicate with each other through radio waves.It has no in built infrastructure.Hence nodes are vulnerable to different types of attacks. So secure routing is an important issue in MANET. In this paper we have proposed a routing protocol based on Optimized Linked State Routing to increase the security level.The protocol is proactive in nature. We have incorporated the concept of trustworthiness of a node along with its reachability factor and battery power in the routing algorithm. Trustworthiness of a node with respect to another node measures what is the probability of successful communication from the first node to the second one.Battery power is also an important factor in MANET since each node has a constant amount of battery power in most of the cases.Reachability of a node is the number of nodes that can be reached from a particular node.More the reachability of a node more is its probability to be chosen by another node as a medium to reach other nodes. The above stated features all together help to choose nodes in a optimum way in the calculation of routing path.



## Keywords

Routing protocol, Proactive , Trust, Fitness, Battery power, Manet.


## 1 INTRODUCTION

MANET refers to a network which is self-configured and is composed of mobile nodes which are connected by wireless links. Each node in the network is mobile i.e. free to move about in any direction. There is no infrastructure (routers, gateways etc) like the conventional networks , in this type of networks. The delivery of data packets is done by the nodes themselves. Hence the nodes act as routers themselves.So routing in Manet is a challenge in itself. Based on when routing tables are built the protocols have been categorized into two divisions

- **Reactive (on-demand) protocols:** These protocols obtain routing information only when needed.
- **Proactive (table- driven) protocols:** Here routing tables are maintained with periodic updation.

Our proposed protocol is an advancement over Optimized Link State Protocol (OLSR) which is a proactive protocol. OLSR is in turn is based upon Link State Routing. In OLSR relay nodes plays an important role in routing.Relay nodes are set of one hop neighbor nodes through which a node can reach to all of its two hop neighbor nodes.In relay node slection the information about the battery power of a node is obtained from the node itself.So a malicious node can advertise wrong information about its battery power.Then there will be high chance of selecting the node as a relay node.AS a result of this routing will be affected.So in our protocol trust factor have been included along with battery power.A node having a minimum amount of trustworthiness and battery power is taken into account for the selection of relay nodes.In th following section the protocol has been described.The future scope of the protocol has been described in the last section.

## 2 SECURE ROUTING PROTOCOL BASED ON FITNESS OF A NODE

An algorithm of a proactive routing protocol has been proposed in this paper (inspired by OSLR protocol).This algorithm uses the concept of trust along with reachability and battery power to choose the multipoint relays of a node in a secured way. Multipoint relay nodes minimizes the flooding of packets to diffuse a message in the network.The different steps of the algorithm have been described in the following subsections.

### 2.1 Neighbour Sensing

Each node in the network sends “Hello” packets in a periodic time interval to get the updated list of its neighbours till two hops. Suppose there are two nodes named A and B. A first sends an empty HELLO message. B receives this message and registers A as an asymmetric neighbour due to the fact that B cannot find its own address in the HELLO message. B then sends a HELLO declaring A as an asymmetric neighbour. When A receives this message it finds its own address in it and therefore sets B as a symmetric neighbour. This time A includes B in the HELLO it


ISBN: 978-81-923777-9-7

sends, and B registers A as a symmetric neighbour upon reception of the HELLO message.

But HELLO messages serve other purposes as well. They are generated and transmitted to all one-hop neighbours to achieve link-sensing, neighbour-sensing, two-hop neighbour-sensing and MPR selector sensing.

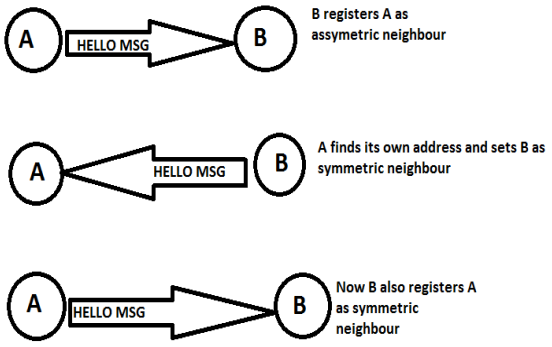


Figure : A typical neighbour discovery session using HELLO messages

The Hello packets are used to update the neighbour table of a node.[1]

## 2.2 Fitness of Node

**Fitness** of a node is a function of battery power of the node. Since the battery power of a neighbouring node is obtained from the node itself. So, there is a probability that the battery power may get tampered. So, the battery power of the node is authenticated by multiplying it with a node's trustworthiness. Fitness is the result value of the multiplication, i.e. Fitness= Trust* Battery Power.It measures the appropriatibility of a node for being chosen as a relay node.

### 2.2.1 Trustworthiness of a Node w.r.t another Node

It is a relative measure between two nodes. It is defined as the ratio of the no. of positive events performed by a node with another node divided by the sum of the number of positive event and negative events performed between the two nodes.

Positive events indicate successful communication and negative events indicates the opposite one.Suppose there exits two nodes A and B and A sends some information to B. When A receives an acknowledgement from B, then it is considered as positive event performed by node B with respect to node A. Any type of successful communication is considered as a positive event. When A does not receive an acknowledgement from B within a certain time interval then it is considered as a negative event performed by node B with respect to node A.Trustworthines of B with respect to A determines what fraction of the communication from B to A has become successful.We have assumed the threshold value for trustworthiness as 0.5.If the trust value is less than it then it has been considered as 0.

### Mathematical Expression for Trustworthiness of a Node

Trust (A, B) =p/ (p+n)

Trust (A, B) is trust of A w.r.t B

p is the no. of positive events

n is the no. of negative events.

The count of the no. of positive events and the no. of negative events is maintained in the routing table.[6]

### 2.2.2 Battery Power of a Node

Battery power plays an important role in relay node selection.In MANET most of the mobile nodes have constant amount of battery power.So relay nodes should be chosen in such away that they have minimum amount of battery power.A trustworthy node without having minimum battery power is of no us since it will become a dead node soon after their selection.We have considered battery power in the range of 0 to 1500.The threshold value for the battery power has been considered as 240 since it has been observed that with battery power below this level a node will not remain active for a reasonable amount of time .Battery power less than this value has been considered as 0.Because with the battery power less than 240 a node will not be available for communication for a reasonable amount of time. [5]

## 2.3 Selection of Relay Node

**Relay _Node(X):-**defines the set of relay nodes for the node X.

1. Initially the trust value between two nodes is assigned 1.

*Algorithm:*

**Step 1:** Start with an empty relay_node(x) set.

**Step 2**: For all nodes in N1(x) calculate n(z,y),where y is a member of N1(x),and z is the no. of the N1 neighbours of y excluding x.

**Step 3**: First select those nodes as relay_node from N1(x) which provides the "only path" to reach some of the nodes in N2(x). [Trivial Case]

**Step 4**: for each node in N1(x)

{

**4.1** At first select the node having $i^{th}$ maximum value for n(z,y).

}

**4.2** Increment I by 1.

**4.3** If the node is not in relay_node(x) then calculate the Fitness of the node. Else go to Step 4.

**4.4** If the value of Fitness is greater than 0.6 then we add the node into relay_node(x). Else go to Step 4.

**4.5** While if some nodes still exists in N2(x) that is not covered by relay_node(x):

Go to Step 4.

Else go to step 4.6.

**4.6** End.

## 2.4 Topology Control

In order to discover the routes to each node from a particular node should have an idea about the topology of the whole network. tC messages are broadcasted through the network. Using TC


ISBN: 978-81-923777-9-7

messages each node updates its topology control table. [3]

The different fields in topology control table are given below:

- Relay_Node IP address
- List of IP addresses that have selected the node as Relay_Node

## 2.5 Routing Table Formation

Each node maintains a routing table where next h op address for each destination is maintained. From the topology control table each node gets the pair of (last_hop,node)where nodes are the addresses found in the topology control table. Suppose node A and B has chosen C as relay_node then for transmitting data to a and B, C will be the second last node. To discover the path between two nodes we backtrack from the destination node to source node using the last hop list.

For example in the following figure if node x wants to find the path till destination Y then it has to find a connected pair [E,Y] then has to backtrack and find the connected pair [D,E] and backtrack until X finds a node which belongs to its relay_node set. Thus the path between two nodes is discovered.

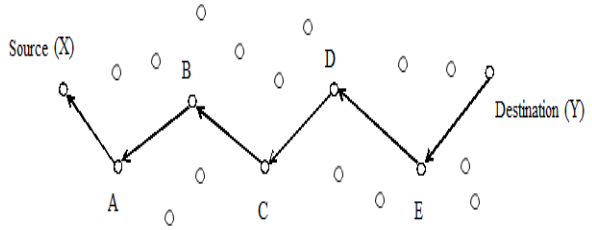


Figure: Source to Destination Route

In the routing table the hop count is also maintained. If more than paths are one path is discovered then the path having minimum hop count is considered as the route.

# 3 CONCLUSION AND FUTURESCOPE

In this paper we have proposed an improvement over Optimized Linked State Routing Protocol by introducing the fitness factor of a node while determining the relay nodes . The fitness function is a function of battery power and trust .Battery power and trust are important parameters in the successful communication between nodes. As we know For mobile wireless network, the performance of a routing protocol is coupled with many factors, like the choice of physical technology, link layer behaviour, etc. The overall behaviour specifies its working domain for which it could be suitable. Since the proposed protocol is proactive in nature, hence it favours the networking context where this all-time-kept information is used more and more and where route requests for new destinations are very frequent. It tries to reduce the burden on the network by reducing the number of broadcasting messages and forwarding the message packets to those which are trustworthy to the sending node. Security is itself incorporated in the protocol by selecting trustworthy nodes as relay node. It also goes in favours of those applications which do not allow long delays in transmitting data packets. It is adapted to the network which is dense, and where the communication is assumed to occur frequently between a large numbers of nodes.

The proposed protocol can be further improved by introducing cryptography which will make the protocol more secure.

# 4 REFERENCES

[1] Clausen T., Jacquet P., Laouati A., Minet P., Muhltahler P., Qayyum A. and Viennot L.,“Optimized Link State Routing Protocol (OLSR)”, IETF RFC 3626, 2003.

[2] Macker J., et Corson S., “Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations”, *Network Working Group rfc 2501*, 1999.

[3]P. Jacquet, P.Muhlethaler, T.Clausen, A.Laouiti, A.Quayyum, L.Viennot “Optimized Link State Routing Protocol for Ad Hoc Networks”, IEEE 2001

[4] Perkins C. E., and Royer E. M., “Ad hoc on-demand distance vector routing (AODV)”, IETF RFC 3561, 2003.

[5] Saaidal Razalli Azzuhri,Suhazlan Suhaimi,K. Daniel Wong "Enhancing the 'Willingness' on the OLSR Protocol to Optimize the Usage of Power Battery Power Sources Left"

[6] “TAODV: A Trusted AODV Routing Protocol for Mobile Ad Hoc Networks”


ISBN: 978-81-923777-9-7