ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

Secured AOLSR protocol for ad-hoc networks using modified Dijkstra's algorithm

Raksha Rao

M.Tech in Computer Networks, Shree Devi Institute of Technology, Kenjar, Mangalore, Karnataka, India

Abstract: Now a days MANETS i.e Mobile Ad-hoc networks is used everywhere all over the world because of its various advantages like portability, reliability, security etc. The main advantage of using this network is a person can contact another person from any place at any point of time. It is not restricted like point to point networks. It is always very important to design well ordered, energy efficient, cost effective, safety etc. In this paper a protocol named Advanced Optimized Link State Routing Protocol is proposed, it uses modified Dijkstra's algorithm as its main logic to find routes in dense networks. This protocol uses appropriate functions which uses weights of link and nodes to find out about the nature of paths whether it is node-disjoint or link-disjoint. Some assumptions are made and analysis is conducted and results are found. The paper tells about characteristics network node and vertex lifetimes, scalability etc

Keywords: Dynamic source routing (DSR); Mobile ad hoc network (MANET); Optimized link state routing (OLSR), Advanced Optimized link state routing protocol;

I. INTRODUCTION

A MANET is a type of ad hoc network that can change locations and configuration of the network at any time. All nodes in this network are mobile and they use wireless connections to communicate with various networks. Topology of Manets is always dynamic and contains many hops. The aim of any network is to reach a remote areas where there is no or fixed communication infrastructures. The major problem in ad-hoc networks are link failures and node failures.

The goals of multipath routing protocol is to balance network load , never compromise the quality of service of the networks and decrease loops in the networks. Few more goals of the multipath routing is to have a minimal delay in the network and increase network lifetime. There are two types of routing protocol i.e. Proactive and reactive in nature. Proactive routing protocols maintain a routing table which stores all the routes of the networks. OLSR is an example for proactive routing protocol. Reactive routing protocol maintains the routing table on demand basis, when there is no demand for that route; it is removed from the table. DSR is an example for reactive routing protocol.

II. CHARACTERISTICS OF MANETS

Here are few fundamental characteristics of mobile ad hoc routing protocols:

- *Distributed routing*: The routing protocol has to be fully distributed, it has to be more fault tolerant. There is no centralised firewall.
- *Adaptive to rapid changes in topology*: Routing must adapt to frequent topological and traffic changes that result from node mobility and link failure.
- *Dynamic*: The nodes can join or leave the network at any point of time.
- *Loop free:* Routes are free from loops. Perhaps to increase robustness, multiple routes should be available between each pair of nodes so that if one of the routes fails, the data can travel via the other paths.
- *All time information:* They provide information to the respective nodes irrespective to their geographical positions.
- *Robust route computation and maintenance*: The smallest possible number of nodes must be involved in the route computation and maintenance process, to result in minimum overhead and bandwidth consumption.
- *Optimal resource consumption:* The devices in Manets mostly run on batteries and are portable devices. Hence it should consume optimal resource i.e. less battery power has to be consumed.
- *Security*: When comparing to wired and wireless network, wireless networks are much more prone for security threats. Hence some form of security protection has to be undertaken so that data is not modified or affected.

III. APPLICATION OF MANETS

When there is any disaster, it is very easy to set up a Manet network than searching for wires or hardware's for a wired communication.

It is commonly used for military purpose where the data has to travel only between soldiers; military headquarters. It can be used when there is need of information exchange by a group of people and many more.

The following figure shows small Manet network.

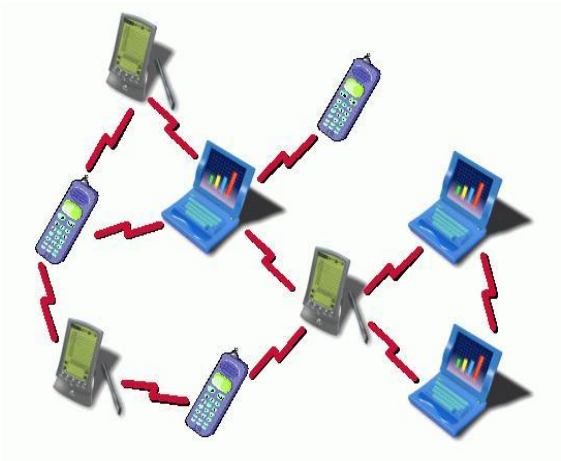
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015



IV. EXISTING METHODS

Two routing protocols for MANET are considered here. One is a reactive routing protocol named as DSR and another one is the OLSR protocol which is a proactive routing protocol.

A. Dynamic source routing protocol

In DSR, It uses source routing rather than using routing table for finding path for intermediate nodes. The mobile nodes maintain the path caches to store the route from source to destination which is updated accordingly as new paths are found from the pre-known source routes. This protocol consists of two functions namely, discovery of path and maintenance of path. When a data packet is to be transmitted to a destination, the source node first determines whether its path is present in the cache already. If a path to the destination is available, the data packet is sent along that pre-stored path. Otherwise, the node starts to find the path by broadcasting Read Request message.

B. Demerits of DSR

- When the nodes are disconnected i.e. no paths in between them, they cannot be reached by this mechanism.
- Entire routing table has to be updated even when there is small change in the network.
- Consumes more time to set the network.
- When there are more mobile nodes, performance is degraded as routing table has to be updated accordingly N number of times.

C. Optimized link state routing protocol

OLSR is proactive in nature. This protocol uses HELLO messages at each node to discover two-hop neighbor information and performs a distributed election of a set of multipoint relays (MPRs). These nodes select multi-point relays such that there exists a path between the neighbours of two-hop and selected MPR. Then TC message is shared between the subset of nodes in the network i.e. only selected MPRs will forward this message which makes this protocol different from other link state routing protocol. MID messages are transmitted by the nodes when there is involvement of network interfaces. This protocol does not send complete routing table in the network. These messages maintain the network topology information under the link failure and mobility conditions.

D. Demerits of OLSR

The following are the disadvantages of using the OLSR protocol:

- Takes more time to discover broken link.
- No provision for multicast of information
- Routing table maintenance, it is of no use to maintain all the routes of the network in the routing table.
- Consumes more resources in order to discover the alternate paths in the network.
- Limited number of control traffic messages
- No security in the network.
- Possibility of network compromise.

V. ADVANCED OPTIMIZED LINK STATE ROUTING PROTOCOL

In this kind of routing protocol, it combines the functionalities of proactive and reactive routing protocols. The routing is made with some proactive routes and then serves the additional routes on demand i.e. reactively. Hybrid routing protocol are employed for large and dense networks because its performance is high in such networks. The topology information is given by sensing of nodes. The estimation of path uses the algorithm called modified Dijkstra's to compute the various paths based on the information from topology detection. Failure of one path or link should not affect the other paths in the network, automatically another link should be chosen till it is replaced.

The flow chart of the protocol is shown in Figure 1.

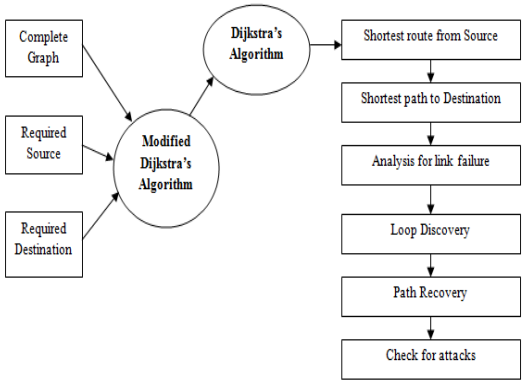


Figure1: Data flow diagram

This protocol takes the entire graph as input and one source and destination from the user. The protocol uses Dijkstra's algorithm to find out the shortest path from given source to all other nodes. Later from the set of paths, the shortest and cost effective path to the given destination is selected. This protocol contains of an additional process known as detection of link, neighbour and topology.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

Detection of links is performed on the basis of the local information of the links such as the cost or weights of the links. Detection of neighbouring nodes is performed by creating a single hop and double hop network which consists all the details of the nodes such as their names, address. The parameters for neighbour detection are energy consumption and hop count. Path determination is done on the basis of demand. The node lifetime and edge life time determines path selection.

VI. MODIFIED DIJKSTRA'S ALGORITHM

The main logic of this protocol is modified Dijkstra's algorithm which is applied to a graph G , two vertices i.e. Src (source), Dest (destination) present in the given graph G , and a positive digits n indicating the cost between the nodes. The algorithm gives set of distance values and path traversed from source to all other nodes. In that optimal and shortest path from required Src and Dest is chosen. The conventions are used in the algorithm:

- *Call_Dijkstra*(*G, Src*) is a function that calls the Dijkstra algorithm and finds out all the shortest distances from source to all nodes of the network.
- *Retrive_Path*(*dist_array*$_i$, *Dest*) is the function to obtain the shortest path to Destination from a distance array of respective required source.

The pseudo code of the algorithm is as follows:

begin
Input the initial graph from user
Input the Src and Dest from the user
for each i=1 to total_nodes-1 do
dist_array$_i$*=Call_Dijkstra(G,Src)*
path_array$_i$*=Retrive_Path(dist_array*$_i$*,Dest)*
//assign weights to the links and nodes
//initial values of Lt_E=0.1 and Lt_N=0.1
for each edge e in G do
$Lt\_E_e=(1-W\_E_e)Lt\_E_e$
end for
for each node n in G do
$Lt\_N_n=(1-W\_N_n)Lt\_N_n$
end for
//this function is used to increase the cost of the edges
for each edge e in G do
if e in path_array$_i$
fun_increase_cost=func_increase_cost(e);
end if
end for
for each node n in G do
fun_increase_weight=func_increase_weight(n);
end for
end for
return path array$_i$
end

Two incremental functions are used to increase the costs of edge and nodes. It uses following weights *W_E (weight of edge)* and *W_N (weight of node)* which is calculated by the following formula.

$W\_E=(L_{t\_max}-L_{t\_min})/L_{t\_avg}$
$W\_N=(L_{t\_node}-L_{t\_thres})/L_{t\_thres}$

Where L_{t_max}, L_{t_min} are the maximum and minimum values of lifetimes of the edges and L_{t_node} is the weight of the node and L_{t_thres} is the threshold value of the node. Based on these values and functions used, the routes can be identified as arc-disjoint or vertex disjoint.

VII. CONCLUSION

The paper proposes a hybrid ad-hoc routing protocol named AOLSR which uses modified Dijkstra's algorithm as its logic. The addition of two cost functions that is increase in cost of the edge and node values of the given graph from required source and destination. The future work involves the enhancement of this protocol in area of security via a partial network topology to detect attacks like spoofing attack, invalid MPR attack, disruption attack, and hop limit attack and drawing the graph selected for the user so that he understands the selected graph effectively.

REFERENCES

[1] Natarajan and Rajendran. EURASIP journal on wireless communication and networking 2014,2014:90 (Base paper of the project).
[2] N Qadri, A Liotta, Analysis of Pervasive Mobile Ad Hoc Routing Protocols, in Pervasive Computing, ed. by AE Hassanien, JH Abawajy, A Abraham, HHagras (Springer, London, 2010), pp. 433–453.
[3] G Cervera, B Michel, GA Joaquin, K Evangelos, Security issues in link state routing protocols for MANETs, in Advances in Network Analysis and its Applications, ed. by E Kranakis. vol. 18 (Springer, Berlin Heidelberg, 2013), pp. 117–148.