Restricted hoping routing protocol

Titu kumar, Rohit kumar jha, Dr.(Prof.) Sitanshu mohan ray

Abstract- Wireless networks are an emerging new technology that will allow users to access information and services electronically, regardless of their geographic position and MANET is a specialization of it. It's is the acronym for Mobile Ad Hoc Network. These networks are made for special purpose and thus resource constraint, easy deployability, fast network functioning and of course security are the major threats of them. In this paper we have discussed a new approach for routing of the data packets. We have substantially decreased the amount of network activity that each node has to make in order to route a data packet. We have furnished algorithms to implement this protocol and exemplified them with a case study. And lastly we have discussed how this protocol is better than the other pre-existing protocols. We can take this paper to its next level, namely "Cognitive Radio" for its futuristic research.

Index Terms— Administrative node, Administrator, Associative node, Common node, Comprenhensive list, Network traffic, Total list, etc.

1 Introduction

Mobile communication is very much different from that of the wired communication. Here the communication is mainly based on the radio signals transmitted by the node. Again characteristics of MANET, also being a wireless network, are quite different from those of the common mobile communication. in mobile communication the nodes mainly use bridge networks within its range to communicate with other nodes. These bridge networks are mainly base stations with whom the source node has to make contact while sending a data packet to its destination. Again we have to remember that these nodes are in constant motion and thus when a node goes out of the range of a base station then it makes contact to its new base station within whose range it falls. This is called Handoff. But in MANET there is no question of base station or any other infrastructure which will be helping to setup or perform the network activity. Thus in this case the nodes are the routers and they have to transfer the data packets themselves. Here comes the essentiality of a very robust and good routing protocol that will perform all the functions but with an optimized network activity which will decrease the network traffic but make the transmission fast. Thus while building our routing protocol we kept in mind this two factors – first is the making the transmission fast and second is the decreasing the network traffic.

In our paper firstly we have described how the entire network will setup from the start, then we have written the algorithms that will implement the protocol. After that we have shown with a case study how the algorithms implement the entire network setup and lastly we have given a comparative note on how this protocol is better than the pre-existing protocols. We have concluded with a conclusion depicting the scopes on which this protocol can be further improved.

2 Scheme

Before we entire into the detailed discussion we have to understand that in a MANET each and every node have a range of itself i.e. it is not possible for any node to transmit the data packet to an infinite distance. Thus the nodes which will fall in the range of a particular node will be called Neighboring nodes. We will interchangeably use friend nodes fro neighbor nodes. They both are same. In the network, there are actually three types of nodes

1. Common nodes
2. Associative nodes
3. Administrator nodes.

This classification is based on the range and the position of each node within a network. To understand classification firstly you have to understand how the entire network is setup.

Each node after a stipulated time period probes who are the nodes that are present in the range of it. when they understand who are the nodes in its neighborhood, they make a list of it and calls it neighborhood list when everyone is done with their neighborhood list. The next work of each node is to check up whether the new list is same with the previous list that it have or not. If the list is same it will understand that no network change has occurred. If any difference is observed the it will report to its administrator. At this point of time, keep it in mind that each node have got a administrator associated with it and that administrator node will always lie in the range of it. now the question is how this administrator nodes are chosen? We will describe it in a few moments. Until now I guess it is understood that each and every node when is idle always probe to see that whether any network topological change have occurred or not around it. if no change had occurred then there is no need to elect new administrator. But if any change had occurred then it is the responsibility of the previous admins to elect the new admins.

Now we will answer how the new admins are selected. Whenever there is a crisis of electing the new admins, all the nodes will send their neighbor's list to their respective admins. The admins will exchange all the neighbor's list among themselves so that each admin have the knowledge of who are the neighbors of each and every node in the entire network. A comprehensive list is made that have the names of all the nodes and their corresponding neighbors written beside them. This list is sorted according to the highest number of neighbors each have. Now we will take all possible one node from the list in top-down sequential manner. For each possibility we will see whether the list containing the names of all the nodes called the entire list is a subset of the neighbor list of that node. If the above proposition is true we designate it as the admin node else we take any two nodes from the comprehensive sorted list in a top-down sequential manner. Now we take the union of the neighbors of the two selected nodes. If the entire list becomes a subset of that we consider those two nodes as the admin nodes. If this time also the entire list does not become the subset we go for taking any three nodes from the sorted comprehensive list in top-down sequential manner and does the same. We continues this process by taking four nodes, five nodes and so forth until the entire list becomes the subset of the union of the neighbor list formed from the selected nodes. Thus the admins are selected.

Now the associative nodes are those which are not admins but they lie in the common region of two or more admin nodes. All the nodes in the network excepting the admins and the associative nodes are the common nodes.

Let us give a small illustrative example of how the admins are selected and which are the admins, associative and the common nodes in that network. This is a small example to have a better understanding. Later in the case study we will describe it in details how from the scratch, when there are no nodes in the network, the entire network is set up and how it works.

The following is the snapshot of the network at a particular instance of time. We will analyze on it

.

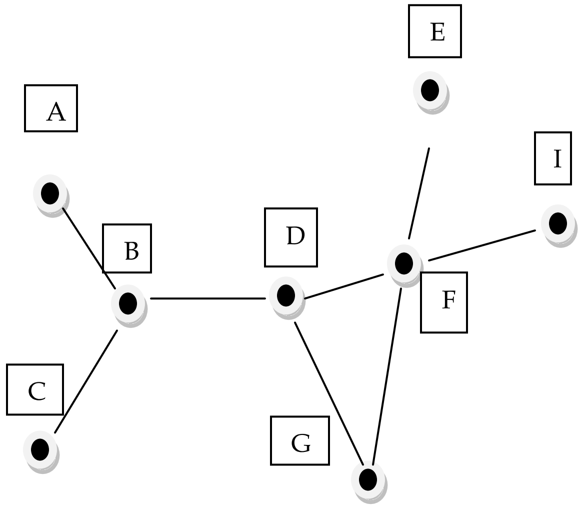

Fig : 1

The following are the comprehensive neighbor's list for each of the nodes (better call it total_list[])

Names of Nodes	Names of the Friends
A	A,B
B	A,B,C,D
C	B,C
D	B,D,G,F
E	E,F
F	D,I,E,F,G
G	D,F,G
I	F,I

Now the sorted comprehensive list is

Names of Nodes	Names of the Friends
F	D,I,E,F,G
B	A,B,C,D
D	B,DGF,
G	D,F,G
A	A,B
C	B,C
E	E,F
I	I,F

Now we blindly assign F as the admin. Its neighbors are D,I,E,F,G. The entire list of nodes are A, B, C, D, E,F,G,I. The neighbors of B i.e. D, I,E,F,G does not cover the entire list. Nor does any of the node from the above list when we take one node at a time. So we consider taking all possible two nodes from the sorted comprehensive list. we observe that for F,B the union of the their neighbor list become A,B,C,D,E,F,G,I. the entire list become the subset of this list. So F,B are selected as the admin. If you think a bit you will admit that we have chosen our admin in such a way that there always will be at least one node that will be common in the neighbor's list of any two of the admin from the selected admins. In our case that common node is D. this d is designated as the associative node as it is associated with both the admins. All the other nodes are considered as the common nodes.

Thus in our case the following are the divisions of the types of different nodes the network have.

Admin nodes: F,B
Associative node: D
Common nodes: A, C,E,G,I

note that the admins are selected as such that all common nodes are in the range of exactly one admin and all the associative node are in the range of at least two or more admins. In our case A,C common nodes is in the range of admin B node and E,G,I are in the range of admin F whereas the associative node D is in the common range of both the admins F,B.

3 ALGORITHM

```
Network change ()    /* this function is probed by every node after a stipulated time period called probe_Timeperiod */
{
for (i=1;i<probe_Timeperiod;i++)
        {
        Make new_friend_list
        If (new_freind_list == my_present_friend_list)
                Stop /* no change in network topology for that node*/
        Else
                Send new_friend_list to my admin
        }
}

Admin_selection_&_routing_info_gathering () /*done by the admins experiencing the change */
{
List_of_all_nodes = Null;
Associative array Total_list[];/* used to contain the names of the nodes and their corresponding friends*/

While (i_get_a_new_friend_list)
        {
        For (i=1;i<time_period;i++) /* time_period= time to send and gather new_friend_list to and from other nodes*/
                {
                set I_am_experiencing_a_change_bit = TRUE;
                send the received new_freind_list to the other admins which are experiencing change;
                }
        Send **request_for_names_of_friend_nodes** packet to other admins;/*will be done  through associative nodes. Note that associative nodes are those who are in the neighborhood of more than one admin node */
        While (reply_of_names_of_friend_nodes packet arrive)
        Total_list[] = decreasingly_sorted(redundancy removed (∑ (all reply_of_names_of_friend_nodes packet) + new_friend_list))/* reply_of_names_of_friend_nodes packet contains the names of all the nodes with their corresponding friend list. This also includes the names of the new_friend_list received by other admins also if any other node's network topological change had occured around them*/
        List_of_all_nodes =redundancy_removed (all the friend of the admin + new nodes in the new_friend_list);
        For (i=1; i< len (total_list[])); i++)
        {
                For all possible combinations of i elements from Total_list[]
                {
                        Adminlist.friend = (total_list[1].friend + total_list[2].friend+ …+Total_list[i].friend)
                        If (List_of_all_nodes are
                        subset of

                   Exit out of this brace;
            }
    }
    Set these combination of i elements from total_list[] as admins in admin_list;
    Associative_node_list =∑( intersection of the friendlist of two admins out of the adminlist but covering all possible combination ;
    Map the associative nodes with the admins comparing the friend list of each admin;

}
```

For routing, a source node sends the data packet to its admin. If found good. Else that admin send it to its associative nodes .if got then good enough. If not it sends it to the other admin. Note that by the definition of associative node it should be having more than one admin around it. Likewise the data packet will be transmitted by admin-associative node-admin hops. One must understand that the network activity is reduced to a lot as the other nodes in the network excepting the admin and the associative are not taking part in the network activity in any case.

4 CONCLUSION

This protocol is best for use of the medium sized and large sized networks. For the small network the computational overhead will be high. It is abest suited when the rate of topological change is medium or slow. For very fast rate of topologicaly changing network it may noy be better than DSR but it will be better than DSDV and also AODV (if in case of AODV the network is not too small). It is true that there are many new advanced protocols that make the transmission rate very high but they have very high computational overhead. This is a protocol which has a optimum network activity, transmission rate and computational overhead

5 FUTURE RESEARCH

We would like to take this paper to its next level, namely “Cognitive Radio”. Cognitive Radio is a wireless network where intelligence is used by the network to dynamically change its parameters for high performance, efficiency and high throughput. IEEE is working on a protocol called WRAN (Wireless Rural Area Network). This protocol is particularly being created for Rural and Remote Telecommunications. This paper on MANET will in the future attempt to use WRAN and create Cognitive Radio Networks that will be used for tapping unused Spectrum from Licensed users through Special algorithms that we will present in our next paper. MANET and Cognitive Radio together will be a huge blessing for Rural India and other Remote regions of the World.

.

5 ACKNOWLEDGEMENT

We are very thankful to Dr. Sitanshu mohan sir for his tiredless support & other reference to prepare our research paper.

6 REFERENCE

[1] [Perkins94] C.E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers" , Comp. Comm. Rev., Oct. 1994, pp.234-244.
[2] [Perkins99] Charles E. Perkins, Elizabeth M. Royer, Samir R. Das, "Ad Hoc On-demand Distance Vector Routing", October 99 IETF Draft, 33 pages.
[3] [Johnson99] David B. Johnson, Davis A. Maltz, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks" October 1999 IETF Draft, 49 pages.

[4]Shukor Abd Razak, Steven Furnell, Nathan Clarke, Phillip Brooke: A Two-Tier Intrusion Detection System for Mobile Ad Hoc Networks- A
Friend Approach, Springer-Verlag Berlin Heidelberg 2006.

[5]Issa Khalil, Saurabh Bagchi,Ness B.
Shroff: MOBIWORP: Mitigation of the wormhole attack in mo bile multihop wireless networks, Elsevier, 2007.

[6]Jianqing Ma, Shiyong Zhang, Yiping Zhong, Xiaowen Tong: SAID: A self-Adaptive Intrusion Detection System in Wireless Sensor Networks, Springer-Verlag Berlin Heidelberg 2007

[7]Yongguang Zhang & Wenke Lee, Proceedings of The Sixth International Conference on Mobile Computing and Networking (MobiCom 2000), Boston,MA, August 2000

[8]Ping Yi, Yiping Zhong, Shiyong Zhang: A Novel Intrusion Detection Method for Mobile Ad Hoc Networks, Springer-Verlag Berlin Heidelberg 2005

[9]Jianqing Ma, Shiyong Zhang, Yiping Zhong, Xiaowen Tong: SAID: A self-Adaptive Intrusion Detection System in Wireless Sensor Networks, Springer-Verlag Berlin Heidelberg 2007

[10]Chai-Keong Toh, "A novel distributed routing protocol to support Ad hoc mobile computing" Proc. 1996 IEEE 15th Annual Int'l. Phoenix Conf. Comp. and Commun., Mar. 1996, pp. 480-86

[11]C.-K. Toh, "Long-lived Ad-Hoc Routing based on the con-

cept of Associativity" March 1999 IETF Draft, 8 pages.

7. AUTHOR'S

1. MR.TITU KUMAR

kumartitu007@gmail.com

2. MR.ROHIT KUMAR JHA

jha.rohit999@gmail.com

3. DR.(PROF.)SITANSHU MOHAN RAY

sitanshuray@gmail.com