International Journal of Research in Advent Technology, Vol.4, No.2, February 2016
E-ISSN: 2321-9637
Available online at www.ijrat.org

Alternating Path Finding using Fast Reroute in Wireless Network

Pragya L.S Balley, Prof. Chaitrali Chaudhari
Department of Computer Engineering, Lokmanya Tilak College of engineering, Mumbai University,
Navi Mumbai, India
*Email:*priya.balley34@gmail.com, chaitralichaudhari@rediffmail.com

Abstract-A wireless ad hoc network is a demoralization type of wireless network. The network is adhoc because it does not rely on a prior infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks [1]. Instead, In these each node of the graph participates in communication for routing by forwarding the data for the remaining other nodes, so the determination of which nodes forward data is made domical on the basis of network affinity. Wireless mobile ad hoc networks are self-configuring ,progressive networks in which nodes are free to move. Wireless networks lack the convolution of infrastructure setup and administration, enabling devices to create and join networks anywhere, anytime [2].In these decentralization nature of the wireless network has make them ethical for using it in number of applications where as overriding nodes cannot be relied on the network [3]. Minimum number of configuration and cursory deployment make ad hoc networks suitable for agile situations like natural disasters or military conflicts. The presence of adaptive routing protocols enables ad hoc networks to be formed expeditious.

Index Terms-Fast reroute; adhoc network ; Routing protocols; alternate routing; wireless network

1. INTRODUCTION

Today the world is rapidly changing and technology is zooming exponentially, the number of users of internet is also increasing rapidly which cause increase in traffic and causes more no of failures in transmission of packets [1]. The backbone process of the global internet or any internal network is Routing .Existing routing techniques includes static and dynamic routing which are implemented using routing algorithms like RIP, EIGRP, OSPF, IS-IS. These routing algorithms intelligently route the packets on the network. There are many scenarios where a packet is sent, the routing algorithm finds an appropriate path for the packet, routes it and it is delivered. There are cases where packets do not get delivered because of many reasons like link failures [4]. A method to find an back up path, after a link failure happened from a source node to a target node is to reroutes the data packet by notifying the sender which takes minimum about 100 mille second. A smarter way to deliver the packet is to reroute the packets from the last successful node.

1.1 Routing

Routing is the process of selecting best paths in a network [1]. In the past, the term routing was also used to mean forwarding network traffic among networks.

1.2 Rerouting

It could cause the route instability and supply the interruption before routing tables at all routers converge to new routes. Fast reroute extensions [2] have been proposed within the IETF to reduce the adverse effects of link or node breakdown by timely invoking the pre-computed repair paths.

1.3 *Module Descriptions*

1.3.1 Topology/Network construction

1. *Node initialization*

This admin will create the network or topology of 5 to 7 nodes by entering the node name, port no, and Ip address.

2. *Network construction*

In this module admin will enter the source name, destination name and node weights for each node for creating the network.

1.3.2 Network Communication

2. *Packet Sender*

In this module sender will select user to which node he want to send the file (In The form of packet).

3. *Shortest Path Generation Algorithm*

In this module the shortest path between the source and destination will be generated and then that path will be displayed.

4. *Routing Table generation*

In this module the by using the shortest path and all the network id, next hop the routing table will be generated.

5. *Packet Receiver*

In this module the destination node will show the received packet and also intermediate path node will receive the packet and displayed.

6. *Link Failure Detection*

Link break between source and destination is analyzed to check path fail. If it is so then that path will be displayed in GUI and the packet will be send on alternate shortest path from source to destination.

2. EXISTING SYSTEM

In our previous works [4], we introduced an IP fast reroute technology for unicast link state routing protocols using the theory of remote LFAP (*Loop Free Alternative* method) to achieve full substitute path analysis under a single link failure with a minimal additional complexity[5].In this scheme ,while the elemental routing protocols detect and react to topology changes in longer time scales. It does not guaranteed to find an alternate route, even if one path already exists.

3. PROPOSED SYSTEM

In these we find alternate method for finding an alternate path during link failure. The current FRR's do not provide an adequate mechanism for technique to re-route packets of link failure. To overcome this a FRR is needed that calculates shortest paths instantaneous .In this method an alternate route is found out instantly after a node Failure, and updating the routing table of other nodes according to the new route.

We are providing the path at the time of node failure or data is not forwarding to other node as it does not communicate. Than new path is provided for communication .For example If source node want to communicate with sink node. but due to link failure the data or packet is not forwarding .At this we are providing the alternate path, we can understand these in given points are such as-

1. Whenever a node fail than instead of going to source node from where the communication is started, It goes to its previous node.
2. Than the previous node choose the other path for communication with sink node.
3. First of it collect all the information of the remaining node.
4. It wait for there response and then communication started.
5. It inform all the node that we have (n-1) path to communicate.
6. Than by applying shortest path algorithm choose the path.
7. So we can say that we have much easier path communication, these can be explain with graph diagram which is given below:-

3.1 Graph diagram

The fast reroute method would establish a new path from the source to destination node in a much lesser time than the existing system do it. Firstly we see the diagram so that we can understand it in a more proper way .Its shown below:-

3.1.1Node description

So: Source Node
A: Node A
B: Node B
C: Node C
D: Node D
E: Node E also attacker node
Si: Sink Node

Hence, we have many paths to reach the destination node from source node (shown in fig 1.0).

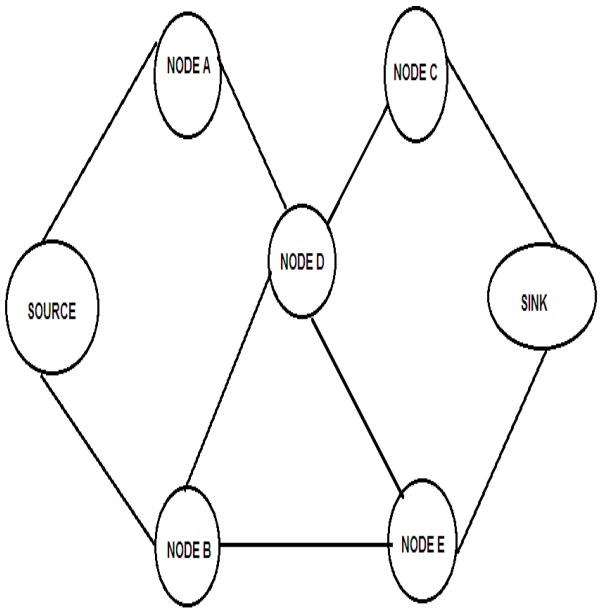

fig 1.0

3.2 Fast route-valid path

First in which communication is done without any dropage of package or data. As according to given

diagram, hope count (number of nodes) here the shortest path will be [source node , node B, node E, sink node].

3.3 Fast Reroute-invalid path

In these we have shown that while communication is going on and they can across a problem that one of the node of the network is not responding, Thus two criteria could be created such as:-

a) In fist case if there is node fail or not responding for much longer time then it could mean that some else attacker is trying to access the data from these node ,thus these is called as attacker node. At these time we can follow the fast reroute method.

b) Second case is that due to some reason it does not follow the path or not able to forward the packet. Than it goes to previous node and communication started again.

- *Example*

Suppose here node E is failed due to some reason than It is known as invalid or attacker path, As it could be possible that may be some else is trying to access the data from network through node E due to which it is not responsing.So node E can be called as attacker node.

3.4 Equal ***cost and multiple path***

One of the oldest and elementary of IP fast reroute techniques is Equal Cost Multiple Path (ECMP) [5], which is an extension enabled in the majority of today's networks. ECMP is usable in those cases when more than one (different) shortest paths are available towards a destination [6].

The traffic is distributed equally among the paths by default, offering increased bandwidth. Additionally, when a failure occurs on one path, routers equity the traffic among the remaining routes. ECMP is easy to implement, but it works only when multiple paths of equal cost are convenient between the source and destination [7].

3.5 Equal cost and multiple path implementation

a) In these method it could choose the path but as we know that we have the problem of choosing the failure path again. thus it increase the time to transfer the packets. we can remove this problem by removing these from the network.

b) So we see that we have remaining (n-1) path for communication.

c) Thus it reduces the time by not going the same path again.

d) We have implemented that we choose the next path on the basis of the time priority which ever generated or activated first has been choose for the communication.

3.6 ***Shortest Path***

Given a vertex, say vertex (that is, a source), this field describes the shortest path algorithm.

The general algorithm is:

1. We will Initialize the array basic Weight so that basic weight[u] = weights [vertex, u].
2. In these set basic weight [vertex] = 0.
3. Find the vertex, v, that is closest to vertex for which the precise path has not been determined.
4. Mark v as the (next) apex for which we get the precise weight.
5. For each vertex w in G, it will be such that the precise path from vertex to w has not been resolve and an edge (v, w) exists, if the weight of the path to w via v is smaller than its current weight, change the weight of w to the weight of v + the weight of the edge (v, w).

4. ARCHITECTURE

The architecture of fast reroute can be shown as:-

.

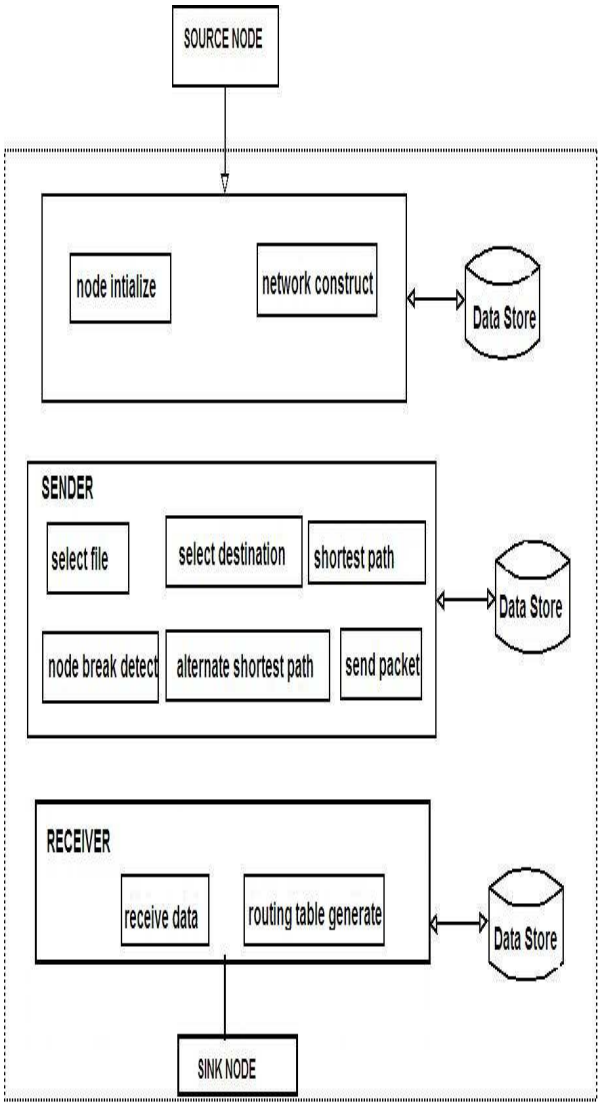

Figure shows the System Architecture

5. WORKING OF THE PROPOSED SYSTEM

In these we have implemented the path for reroute in case of node failure. Process does not stop it further go back to its previous node. From there retransmission of the data packet is initiated .It does not go to source node again.

5.1 *Rerouting mechanism*

We decided one node as Attacker node

1. First create the network structure.
2. Identify source and destination node.
3. Identify neighboring node connectivity for each node as edges
4. For each edges of source node e
5. Initialize total weight = weight of current edge(=1)
6. Initialize min_ weight as infinity
7. set v as next node of edge e
8. Set path = source, v
9. while v is not destination
10. Set f as next edge of v
11. Add weight of f to total weight
12. set v as next node of edge f
13. append v to path
14. end while
15. if total weight < min_ weight then
16. min_ weight = total weight
17. min_ path = path
18. end if
19. end for
20. Then transmit data on selected min_ path
21. If we choose the attacker status in attacker node then if we find the attacker node in path then packet is send back to its previous node
22. choose another path at previous node and packet is sent to destination from other node.

5.2 *Rerouting description*

We decided one node as a Attacker node i.e Node E

1. First create the network structure.
2. Then choose the source node and destination node.
3. Then we find the shortest path between them using shortest path algorithm.
4. Then select txt file to send between them.

If we choose the attacker status in attacker node then if we find the attacker node that is Node E in path then packet is send back to its previous node and then choose the another path and packet is sent to destination.

Then the packet is sent from this path and received at destination node destination node and source node receives the response also.

6. CONCLUSION

We presented various network designs and backup reconfiguration schemes for restoring multiple failures using FRR. These are the first designs with formal (worst case) guarantees of no loss of connectivity. Although our proofs of correctness are complex, the descriptions of the designs and protocols are simple. Using a lower bound argument, we showed that one of our constructions is nearly optimal in the number of edges. A numerical evaluation showed that, e.g., a

network graph with average degree 7 with 57% overbuild can support failures of up to 4 edges.

We also conclude that we do not required the expensive infrastructure, communication is possible in much easier way. In these information is distributed so ,By providing the path (n-1).It saves the time by not following the same path in which node failure is found.

7. FUTURE SCOPE

In future the implementation can be made more optimize .The load which come on the previous node at the time of node failure, It could be decrease by giving the prior information from the source node to the previous node of whose prior node is failed (here previous node is D ,whenever node E is failed than all the transmission started from node D) that how many remaining neighboring nodes are connected and able to transfer the packet or data.

REFERENCES

[1] A. Atlas, Ed.,"U-turn alternates for IP/LDP fast-reroute,"IETFdraftatlas-ip-local-protect-uturn-03, Feb. 2006.

[2] A. Atlas and A. Zinin, Eds., "Basic specification for IP fast reroute: loop free alternative," IETF RFC 5286, Sept. 2008.

[3] S. Bryant, C. Filsfils, and M. Shand, "Remote LFA FRR," IETF Internet Draft draft-shand-remote-lfa-00, Oct. 2011.

[4] C. Filsfils and P. Francois, Eds., "Loop-free alternative (LFA) applicability in service provider (SP) networks," IETF RFC 6571, June 2012.

[5] E. M.Gafni and D. P. Bertsekas,"Distributed algorithms for generating loop-free routes in networks with frequently changing topology," *IEEE Trans. Commun.*, vol. COM-29, pp. 11–18, 1981.

[6] I. Hussain, *Fault-Tolerant IP and MPLS Networks*. Cisco Press,2005.

[7]A. Kvalbein, A. F. Hansen, T.ˇ Ciˇci´c, S. Gjessing, and O. Lysne, "Multiple routing configurations for fast IP network recovery," *IEEE/ACM Trans. Netw.*, vol. 17, pp. 473–486, 2009.

[8] K. W. Kwong, L. Gao, R. A. Gu´erin, and Z. Zhang, "On the feasibility and efficacy of protection routing in IP networks," *IEEE/ACM Trans. Netw.*, vol. 19, pp. 1543–1556, 2011.

[9] S. S. Lor, R. Ali, and M. Rio, "Recursive loop-free alternates for full protection against transient link failures," in *Proc.2010 IEEE Symp. On Comput. and Commun.*, pp. 44–49.

[10] G. R´etv´ari, J. Tapolcai, G. Enyedi, and A. Cs´asz´ar, "IP Fast Re Route: loop free alternates revisited," in *Proc. 2011 IEEE Int. Conf. on Comput. Commun.*, pp. 2948–2956.

[11] J.M.Welch and J.E. Walter *Link Reversal Algorithms*. Morgan & Claypool Publishers, 2012.

.