IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 4, Issue 1, Feb - March, 2016
ISSN: 2320 – 8791 (Impact Factor: 2.317)
www.ijreat.org

Reroute Packets To The Nearest Node Using Floyd's Algorithm

Malini.S, Mohana.B, K.Jaisharma

COMPUTER SCIENCE AND ENGINEERING, G.K.M. COLLEGE OF ENGINEERING AND TECHNOLOGY, CHENNAI, INDIA

ABSTRACT

An important problem in IP networks is to check that any topology changes do not put off network performance. IP Fast Reroute (IP FRR) is a scheme to address this issue by exactly forwarding an IP packet to a predestined equivalent next-hop when the primary next-hop to the destination goes unavailable. A systematic and effective IP FRR scheme called DisPath, is employed to identify the equivalent next hop towards destination by finding the minimum cost. DisPath assures full coverage, guard against failure of node(s), with low complexity and minimum estimation cost. DisPath generally creates minimum-cost alternative paths than other schemes adopted by the industry. Combined with the preceding security guarantee and implementation in simple way, these results provide strong proof that DisPath is a most fascinating choice of IP FRR scheme.

KEYWORDS: DisPath, IP FRR, Minimum-cost, Predestined

1. INTRODUCTION:

Networking is the practice of interfacing two or more computing device with each other for the purpose of sharing information. Computer network is a combination of hardware and software. Computer networks can be classified into different types.

1.1 LOCAL AREA NETWORKS (LAN)

A LAN is a group of computers and network communication devices within a limited geographic area. No third party involvement is required. They are symbolized by the following:

- Data transfer speed is high,
- Low cost technologies,
- Limited geographic area.

1.2 WIDE AREA NETWORKS (WAN)

A WAN is a combination of LANs. It is not confined to a particular geographic area and may be linked around the world. Third party network is required. They are represented as:

- Many interconnected LANs
- Usually more expensive technology
- More refined to implement than LANs
- Unlimited geographic area
- Less error detention due to transmission distances

1.3 ARCHITECTURE OF NETWORKING

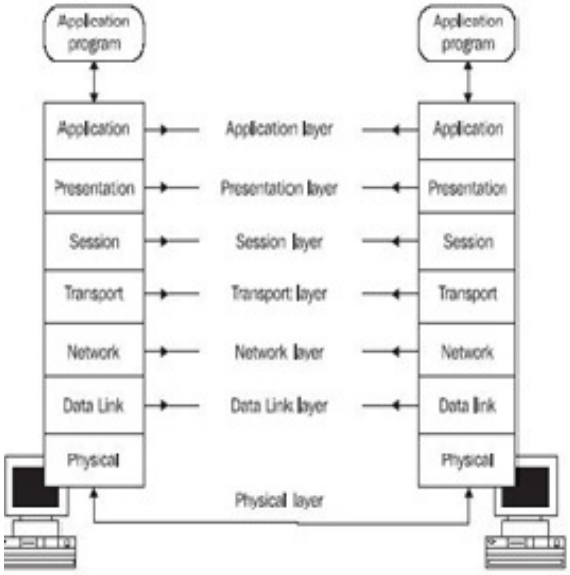

Fig 1: NETWORK ARCHITECTURE

1.3.1 APPLICATION LAYER

It is the application that is used to access the network. Each application performs something specific to the user needs, e.g. browsing the web, transferring files, sending email.

1.3.2 PRESENTATION LAYER

The prime functions of the presentation layer are data formats, encryption/decryption of data, and compression/decompression of data.

1.3.3 SESSION LAYER

It specially deals with access rights in setting up sessions, e.g. who have access to particular network services, credit functions, etc.

1.3.4 TRANSPORT LAYER

The network layer provides end-to-end packet pipe to the transport layer, the transport layer renders end-to-end message service to the top layers.

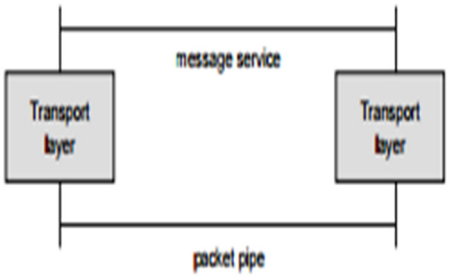

Fig 2: FUNCTIONS OF TRANSPORT LAYER

Transport and network layers Functions of the transport layer includes:

• Breaking messages into packets and reassembling packets into messages (packets of suitable size to network)

• Re-arranging packets at destination to retrieve correct sequence (e.g. Datagram)

• Acquiring end-to-end reliable communication if network is not reliable, recover from errors and failures (arbitrary networks can join the Internet!)

• Flow control to protect a fast sender from overrunning a slow receiver Example of transport protocols for the Internet or Transmission Control Protocol and User Datagram Protocol. When combined with the IP protocol at the network layer, we call TCP as TCP/IP.

1.3.5 NETWORK LAYER

The main function of the network layer is to route each packet to the proper data link control or to the transport layer (if the node is the destination). Generally, the network layer computes its own header to the packet received from the transport layer to achieve this routing function.

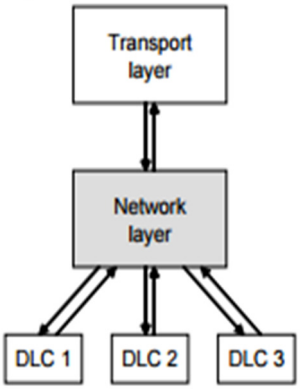

Fig 3: TRANSPORT LAYER FUNCTIONS

1.3.6 DATA LINK LAYER

The Data Link layer is constrained for transmission of packets without errors in a single link. The goal is to check whether every packet is delivered only once, without errors and in order. To accomplish this task, Data Link Layer adds its own header/trailer. For instance, the header may contain sequence numbers to ensure delivery of packets in order. The packet, thus modified is called a frame.

1.3.7 PHYSICAL LAYER

The physical layer is responsible for the original transmission of bits in a link. This layer is usually the network hardware. Higher layers, like Data Link Layer, must deal with transmission errors due to noise and signal power loss. An efficient model for the physical layer is the Binary Symmetric Channel(BSC) with a probability p of twisting each bit independently, i.e. $p\{0 \rightarrow 1\} = p\{1 \rightarrow 0\} = p$. However, in practice errors are busty.

2. METHODOLOGY:

2.1 DISPATH SCHEME

In a bi-connected graph every node x as two disjoint path to a given destination y. Example: Given a directed graph **G=(V,E)** with source **s ∈ V** and sink **t ∈ V**, where edge **(u,v) ∈ E** has capacity **c(u,v)> 0**, flow **f(u,v)≥0** and cost **a(u,v)**. The cost of sending this sequence is **f(u,v).a(u,v)**. It is required to send an cost of flow **d** from **s** to **t**. The problem here to find the minimum cost:

$$\sum_{(u,v) \in E} a(u,v).f(u,v)$$

Fig 4: EXAMPLE FOR MINIMUM COST TREE

2.2 DESCRIPTION

Dispatch algorithm includes three steps

Step 1: Sink tree computation. Node x estimate the sink tree that is common to all nodes the parent of x is noted as the primary neighbor

Step 2: Manipulation of weight it reduces the weight of links

$$w_t(e) = \begin{cases} (1-\varepsilon)\cdot w(e), & \text{if } e \in T(t) \\ w(e), & \text{otherwise.} \end{cases}$$

Step 3: Shortest path computation. Node x calculates shortest path with respected weight using dispath algorithm the failure of anode makes all links to that node to become unavailable and it doesn't distinguish between node failures and link.

2.3 ALGORITHM

1. The Floyd algorithm is used where the shortest path between all pairs of nodes is estimated.

2. Update all shortest paths that include the node as an intermediate vertex in the shortest path.

3. Floyd's algorithm is an approach that is exhaustive and incremental. The entries of the A-matrix are updated every time a[i, j] is compared with all possibilities, that is, a[i, k] + a[k, j], for $0 \leq k \leq n - 1$

4. For every pair of nodes (i, j) of source and destination vertices respectively, there are two possible cases.
1) If k is not an intermediate vertex in minimum cost path from i to j, then keep the value of distance[i][j] as it is.
2) If k is an intermediate vertex in minimum cost path from i to j, then update the value of distance[i][j] as distance[i][k] + distance[k][j].

3. TECHNICAL GLOSSARY

- **MULTIPROTOCOL LABEL SWITCHING (MPLS)**

  MPLS is a mechanism in telecommunications network, that is of high-performance, directs data from one network node to the next using the shortest path costs rather than network addresses' length, avoiding complex search in a routing table.

- **LINK-STATE ADVERTISEMENT (LSA)**

  LSA is a basic communication based on OSPF routing protocol for the Internet Protocol (IP). It transfers the router's local routing topology to all other local routers in the same OSPF network coverage.

- **INTERIOR GATEWAY PROTOCOL (IGP)**

  An interior gateway protocol (IGP) is a type of protocol used for interchanging the routing information between gateways in an autonomous system (say a system of corporate networks in local area). Then this routing information can be used to route network-layer protocols like IP.

4. DISCUSSION:

4.1 EXISTING SYSTEM

- IP Fast Reroute in which forwarding the packets to equivalent next-hop as soon as the primary next-hop to the destination becomes unavailable.
- IP Fast Reroute (IP FRR) scheme introduces the DisPath in which it leverages the fundamental properties of the node-disjoint paths.
- All routers maintain link state information that allows them to calculate the network topology.
- An IP FRR scheme that provides protection against any single link or node failure in a network.
- IP FRR approaches, which minimize network service disruption during convergence periods.

4.2 PROBLEMS IN EXISTING SYSTEM

- IP Fast Reroute in which forwarding the packets to equivalent next-hop as soon as the primary next-hop to the destination becomes unavailable.
- The packets will send from source to destination in network topology.
- The DisPath in which, while sending the packets if any link failure occurs, it will make the equivalent path to reach the destination.
- If any failure occurs and is detected, only adjacent routers are aware of it, and this process is called the local repair routers (LRR).

4.3 PROPOSED SYSTEM

IP Fast Reroute in which forwarding the packets to equivalent next-hop as soon as the primary next-hop to the destination becomes unavailable. The packets will send from source to destination in network topology.

- The DisPath in which, while sending the packets if any link failure occurs, it will make the equivalent path to reach the destination.
- If any failure occurs and is detected, only adjacent routers are aware of it, and this process is called the local repair routers (LRR)
- In the proposed, we are going to implement through the Floyd's algorithm.

4.4 ADVANTAGES

- It will have the much easier to code.
- It is used to find the all pairs of the shortest path throughout the network.

5. CONCLUSION:

This paper includes Floyd's Algorithm, an IP Fast Reroute scheme that provides security, in a network, for any single node or link failure. Along with the initial requirements on the routing table that holds the minimum cost i.e., the value of each node from every other nodes, it ensures low computational value and less complexity. This approach can be easily applied on existing/available routers. Above that, the outcome of this method is proved to be very competitive in accordance to the stretch of the nodes as well. The simplicity to implement, full network coverage, and the node stretch factor made us to understand that our approach is a solution for strong practical IP FRR.

6. ACKNOWLEDGEMENT:

We would like to express our sincere gratitude and greatest respect towards Assistant Professor K.JAISHARMA for giving us an opportunity and guiding us to complete the project in time.

7. REFERENCES:

[1] A. Atlas, Ed., "U-turn alternates for IP/LDP Fast-Reroute," IETF, Internet-Draft, 2006.
[2] A. Atlas and A. Zinin, Eds., "Basic specification for IP Fast Reroute: Loop-free alternates," IETF, RFC 5286, 2008.
[3] K. Xi and H. J. Chao, "IP fast reroute for double-link failure recovery," in Proc. IEEE GLOBECOM, 2009, pp. 1-8
[4] X. Yang and D. Wetherall "Source selectable path diversity via routing deflections" in Proc ACM SIGCOMM, 2006, pp. 159–170.
[5] Z. Zhong et al., "Failure inferencing based fast rerouting for handling transient link and node failures," in Proc.IEEE Global Internet Symp., 200