ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Survey of Multipath routing Methodology based on (Independent Directed Acyclic Graph) IDAG

Mr.Prashant Rewagad [*1], Mr.Hiralal B. Solunke [2]
[*1,2] Department of CSE , GHRIEM,Jalgaon, India
prashant.rewagad@raisoni.net

Abstract

In Networking when packet is send from source node to the destination node, there are different types of problems are occurred in path of that particular packet, that is Node Failure or Link Failure and many more, the result is that increasing of network traffic or Congestion & there is also the problem that packet not deliver to the node. To overcome these in networking to achieve the Multipath routing or Multipath Routing is very important, there are different things are available but the best result can be achieve with the help proposed system that is Yet Another Multipath Routing . In other Routing Mechanism packet dropping & Packet Redirection, Delay , is available, to overcome these Yet Another Multipath Routing scheme is Best. The algorithm in our system provides the: i) Multipath Routing with Network Efficiency, ii)Backup Link, iii)Packet Redirection, iv)Decrease the Packet Delay, V)Provides SECURITY.

Keywords: Introduction, Existing System, Conclusion, & References..

Introduction

The Multipath Routing it is a mechanism in which the packet is transferred from source to destination with multiple available path**.** It means that it provides the multiple available links to the packet in case of node failure. Generally we can say that multipath routing is the spreading of traffic from a source node to a destination node over multiple paths through the network.

Multipath routing is the routing technique of using multiple alternative paths through a network, which can yield a variety of benefits such as fault tolerance, increased bandwidth, or improved security.The multiple paths computed might be overlapped, edge-disjointed or node-disjointed with each other.Multipath routing is a promising routing scheme to accommodate these requirements by using multiple pairs of routes between a source and a destination. With the scheme, we can achieve robustness, load balancing , bandwidth aggregation , congestion reduction, and security compared to the single shortest-path routing that is usually used in most networks. Multipath routing in today's IP networks is merely limited to equal-cost multipath. Techniques developed for multipath routing are often based on employing multiple spanning trees or directed acyclic graphs .

Suppose we want to send a packet from from source to destination. The Particular packet is travelled from different node and different links, and reach to the intended destination, But what will be the solution when particular node is failure or particular Link is Failure, The Solution is Mutipath Routing with Network Efficiency.

Existing system

This part Describes the what are the proper analysis of the existing systems, means whether the existing systems provide better advantages to the customer or not.

The brief Description of different Multipath algorithms is described below:

1) In this **Sangman Cho *et** al* describes that send the packet to the intended destination by independed link and the independent node,The advantage of this methodology is that it saves the packet from dropped and failure in case of link & intended destinations[1].The Disadvantages of this methodology is it does not provide the multipath routing with network efficiency & does not provides the Security to the intended packet[1][2]. The Concept this methodolgy can be understood from the figure 1.

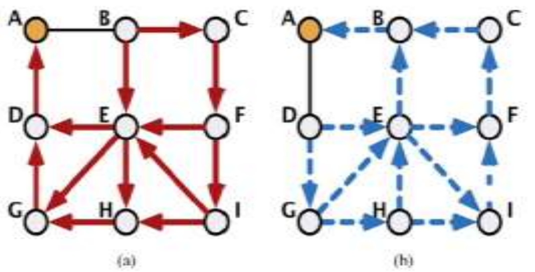

Fig 1.Illustration of node-independent DAGs in an example network where node A is the root (destination) node. (a) Red DAG. (b) Blue DAG.

The above diagram describes that the if particular node or link is fail at that time the recovery is possible from that.

2) The Next methodology is by **Shree Murthy *et al,*** Here they develop the multipath routing mechanism for connection less network ,that dynamically adapts the congestion.In this techniques the packet forwarding is done by hop-by-hop mechanisms & every node is act as a PGPS server which contains the destination-based permit bucket[3].

This methodolgy uses the concept of Traffic Shaping by permit buckets,Traffic Separation,All paths are loop free.This mechanism is very useful this concept can be understood from the following Figure 2.

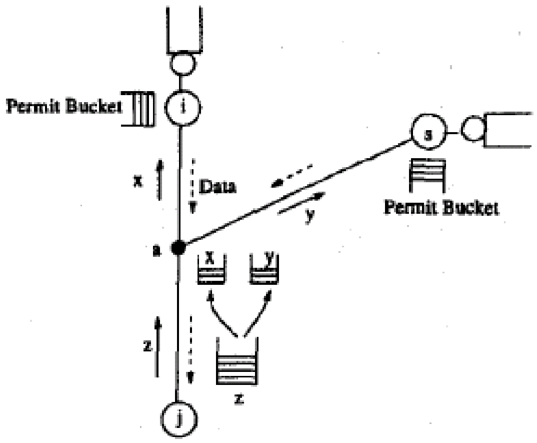

Fig 2.Congestion oriented multipath routing.

The Figure 2 Describes that the when lots of packets are reached at he node to node there are many chances that the Node may go in a congested mode, so to overcome this the mechanism is that the permit bucket is used to overcome the congested area that advantages of this methodology as it name suggest that congestion is managed and the disadvantages is that the extra permit bucket is required to perform the better multipath routing.

3) Here now we described that the another methodology by the **Israel Cidon**, *et al* ”In this paper author analyse the multipath routing mechanism in which they show the multipath routing is best persistent than the single path [3].

It means that the multipath routing is better than the single path routing because if in any case the node is fail or link is fail at that time the whole network is lost but for multipath routing no any chances of network fail because that the multiple path is available .The main fundamentals aspects the author described is as described below:

Three sub-families of algorithms are presented in.

a)Fast algorithms: where the reservation message travels to the destination as fast as possible, but the best possible route might not be the one selected

b)Slow algorithms: where the reservation message travels to the destination at the speed of the slowest path, but the selected path is guaranteed to be the best in the diroute and the message complexity is linear in the number of diroute links.

c) Superfast algorithms: where the reservation message from the source to the destination and the positive acknowledgment From the destination to the source, both travel as fast as Possible. Similar to the fast algorithms, the selected path might not be the best. The superfast algorithms use initial multicast connections that are gradually pruned to a unicast connection. The main thrust of the algorithms is to reach the destination with a feasible path (using a flooding-like approach), altering the path if better alternatives are found in time, and releasing superfluous reserved bandwidth as soon as it is identified.

The forward flooding is implemented by Request messages that carry the cost of the sub-route from the source to the node they arrive at. This cost is used by the intermediate node to select the best current incoming sub-route if several exist, and to release the resources from the rest. Only a single reservation in made in a link even if it is shared by several sub-routes.

A destination node that receives, at least, one message starts the second stage of the algorithm by sending an message. This message travels backward along the reserved route and fixes its selection, i.e., a node that receives an message cannot change its sub-route selection anymore. In the super-fast algorithm, there is an additional backward flooding message to signal the source that a route has been found and that data transmission can be started .

These algorithm represent different tradeoffs between the speed the search advances and the quality of the resulted route. All of them use the early-release mechanism to release redundant resources (bandwidth) as soon as possible. We expect this work to trigger future development of multi-path reservation algorithms.

Finally In this This paper author analyzes the performance of multi-path routing algorithms that reserve resources along the paths considered for routing. The analysis is based on the Poisson model which is no longer used for packet-level analysis, but is still considered a good estimation of the burst (or session) level analysis presented in this paper. Also unlike packet generation where an ON-OFF model is considered a common extension to the Poisson, there is no general consensus on alternative bursty call generation processes or even if it is required. This is a very interesting open question. Note that in this abstraction level, the independence assumption is also a good estimation.

4)The Another methodology is that the methodology in which the Single node Failure or Single link Failure,how that the algorithms are works can be understood from the following discription.

Kang Xi ,*et al*- In this paper authors investigates the existing algorithms & find out a new way to fast Recovery from the link failure & Node failure by calculating the **backup paths** in advance.[4]

Failure recovery in IP networks is critical to high quality service provisioning. The main challenge is how to achieve fast recovery without introducing high complexity and resource usage. Today's networks mainly use route recalculation and lower layer protection. However, route recalculation could take as long as seconds to complete; while lower layer protection usually requires considerable bandwidth redundancy. They present two fast rerouting algorithms to achieve recovery from single-link and single- node failures, respectively. The idea is to calculated backup paths *in advance*. When a failure is detected, the affected packets are immediately forwarded through backup paths to shorten the service disruption. This paper answers the following questions: 1. How to find backup paths? 2. How to coordinate routers during the rerouting without explicit signaling? 3. How to realize distributed implementation?.

The schemes react to failures very fast because there are no calculations on the fly. They are also cost efficient because no bandwidth reservation is required. Our schemes guarantee

100% failure recovery without any assumption on the primary paths. Simulations show that our schemes yield comparable performance to shortest path route recalculation. This work illuminates the possibility of using pure IP layer solutions to build highly survivable yet cost-efficient networks.

The Concept of IP Fast Re-routing can be understood from the following Figure 3.

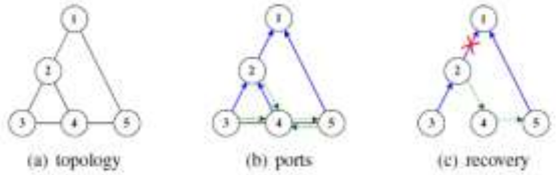

Fig 3: Example of IPFRR (solid/dashed arrows are primary/backup ports).

Each IP router maintains a primary forwarding port for a destination (prefix). When a failure occurs, some of the primary ports could point to the damaged link/node and become unusable. The idea of IPFRR is to proactively calculate backup ports that are used to replace primary ports temporarily until the subsequent route recalculation is completed. Figure 3 shows an example with node 1 as the destination. Figure 3(a) is the topology, Figure 2(b) shows the primary and backup ports, and Figure 3(c) shows the recovery where node 2 and 4 switch to their backup ports. Figure 4 shows that IPFRR resumes disrupted services immediately after a failure is detected while route recalculation is performed in parallel.

The Figure 4 is show below:

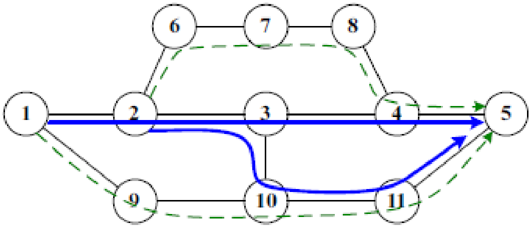

Fig 4. Link-disjoint paths (solid/dashed lines are primary/backup paths.

Finally the conclusion of this methodology is that the author study IP fast rerouting (IPFRR) under single-link and single-node failures. The first contribution of this work is that the problems are formulated as integer linear programming (ILP), which can be easily extended to support various design objectives and constraints. Our second contribution includes two IPFRR schemes that guarantee 100% recovery from single-link and single-node failures, respectively, which they call ESCAP. The schemes have low complexity and can be easily applied to practical networks to substantially shorten service disruption caused by failures. We verify the performance of our schemes in a variety of practical and random topologies and show that the price paid for the survivability enhancement is insignificant. The path lengths, link load and network overall traffic volume using our schemes are comparable to those using shortest path route recalculation.

5) Now finally the best methodology by the **Igor Ganichev *et al*** ,The methodology they described which is nothing but the Yet another multipath routing mechanism.[5]

Multipath routing is a promising technique to increase the Internet's reliability and to give users greater control over the service they receive. However, past proposals choose paths which are not guaranteed to have high diversity. The author propose yet another multipath routing scheme (YAMR) for the interdomain case. YAMR provably constructs a set of paths that is resilient to any one inter- domain link failure, thus achieving high reliability in a systematic way. Further, even though YAMR maintains more paths than BGP, it actually requires significantly less control traffic, thus alleviating instead of worsening one of the Internet's scalability problems. This reduction in churn is achieved by a novel hiding technique that automatically localizes failures leaving the greater part of the Internet completely oblivious. There are two methodology used by these techniques they are YAMR path Construction & Hiding route updates.These concepts are described below:

A)Yamr Path Construction:-

This component of YAMR (which call YAMR Path Construction, or YPC) computes a set of alternate paths that are deviations from BGP's default path.2 Each alternate path is computed assuming that a link in the default path is down. Considered as a static set of paths, there is no single failure that can break all the paths simultaneously, unless that failure disrupts all policy-compliant paths between the source and receiver. When protocol dynamics are taken into account, the story is more complicated (because when BGP recovers from a link failure, it can break paths that did not contain the failed link).

YAMR present simulation results on the actual resilience achieved under full dynamics, which show that YAMR improves the reliability of BGP in single link failures by almost three orders of magnitude. However, computing this family of paths involves higher control plane messaging overhead than BGP. Therefore added another component to YAMR.

Generally we can say that the YPC or YAMR Path Construction it is the mechanism which is used to construction of the available path efficiently.

The concept of the YPC can be understood from the following figure 4.

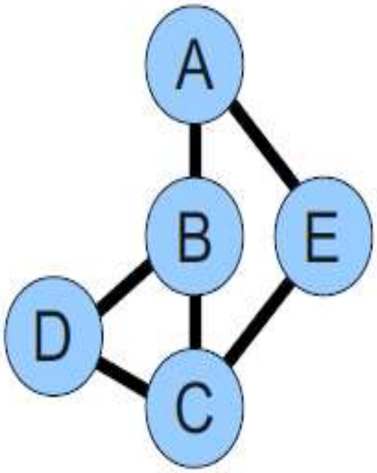

Fig. 4:YAMR YPC Path Construction

The complete run of YPC shown in Figure 4 . First, C announces its default path [C] to its neighbors, which then construct their default paths. None of the neighbors is able to construct an alternate path yet. Next, B and D send their default paths to each other. Upon processing these messages each is able to construct the alternate path it needs. Next, B and E send to A the updates to their RIB LOCALs. A can construct its default paths either from [B,C] or [E,C]. A prefers to have [A,B,C] as its default path and now needs to construct alternate paths avoiding links (A,B) and (B,C). For the (A,B)-avoiding path A has the path [A,E,C] as the only choice because the path [A,B,C] goes through (A,B) and the path [A,B,D,C] cannot be considered because of its label (and would be unsuitable anyway, since it does not avoid (A,B)).

B)Hiding Route Updates:-

Hiding Route Updates is a mechanism in which as it name suggest hiding route updates means that it updates the route according to the current situation for the respective packet. It means that it any node is fail or any link is fail which is to treated as a faulty link or faulty node and that node or particular link hided & when any live node wants to send the packet at that time that affected particular node or link not considered for the packet transmission. YAMR's hiding technique is a set of distributed mechanisms that can be applied to either YPC or BGP to confine the effects of a link failure to a small neighborhood around the link. Hiding A Ses do not propagate information about the failure to their neighbors if they can safely reroute around it. For example, in Figure 3.2.1, if link (B,C) fails, B can reroute around this failure by deflecting all traffic onto [B,D,C] without telling A that path [B,C] has failed. We call B a hiding AS, path [B,D,C] a deflection path, and path [B,C] (the failed path being hidden) a lame path.

The Concept of Hiding Route Update scan be understood from the following diagram Figure 5.

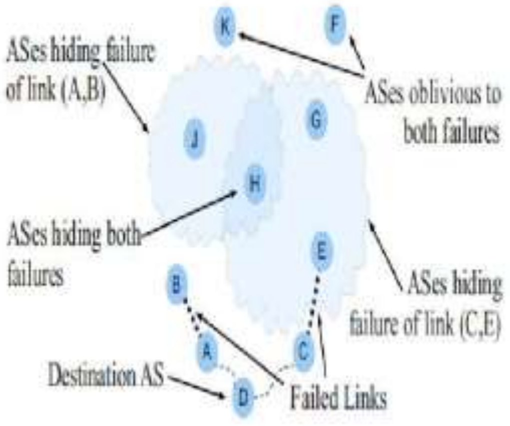
ASes hiding failure of link (A,B)
K
F
ASes oblivious to both failures
J
G
H
ASes hiding both failures
E
ASes hiding failure of link (C,E)
B
A
C
Destination AS
D
Failed Links

Figure 5 An illustration of Hiding Bubbles.

In the figure 5 above, *B* is able to completely hide the failure so that all other ASes remain oblivious to it. However, in general topologies and policies, *B* might be able to hide the failure only from a subset of its neighbors, but can't hide it from others because it doesn't have a suitable path it can export to them. In such a case, *B* withdraws the failed path from the neighbors for whom it can't hide the failure. These neighbors then try to hide the failure from their neighbors, recursively. This process continues until the failure is completely hidden. In other words, a single failure is hidden by a dynamically determined bubble of hiding ASes This can be understood from figure 4 above figure .

Conclusion

Finally we conclude that the multipath routing it a way to provide the available path to the packets, There various techniques and methodology are described above they are have various advantages and there intended limitations.

First discussion is that the multipath is achieve by with the help of the independent node and independent link the algorithm used here it is polynomial time algorithm, the disadvantages is security,& Packet dropping.

Second discussion is that the provides the multipath availability in the congested environment but the disadvantages is here the extra permit bucket is required to handle the packet it acting as a buffer.

Next discription is that the analysis of existing algorithm and they develop the methodology means another algorithms i.e. Fast algorithms, Slow algorithms and superfast algorithms

Next Discription describes that the IPFRR it IP Fast Rerouting in Single Link failure or Single Node Failure.

Finally the best methodology is YAMR in which YAMR Y path Construction & Hiding Route Updates. The mechanism, YPC, to systematically construct a set of paths that is resilient to any one link failure. Because YPC manages more paths than BGP, it has a higher churn and a longer convergence time. However, when YPC is combined with the hiding technique, churn and convergence time fall well below the BGP levels. In our trials, YAMR increased the reliability by almost three orders of magnitude.

Finally the YAMR Mechanism is best than the existing Methodology.

References

1. *Sangman Cho, Theodore Elhourani, and Srinivasan Ramasubramanian, "Independent Directed Acyclic Graphs for Resilient Multipath Routing," IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 20, NO. 1, FEBRUARY 2012.*
2. *Sangman Cho, Theodore Elhourani, Srinivasan Ramasubramanian, "Resilient Multipath Routing With Independent Directed Acyclic Graphs".*
3. *Israel Cidon, Raphael Rom, and Yuval Shavitt, "Analysis of Multi-Path Routing," IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 7, NO. 6, DECEMBER 1999.*
4. *Kang Xi and H. Jonathan Chao "IP Fast Rerouting for Single-Link/Node Failure Recovery".*

5. *Igor Ganichev, Bin Dai , P. Brighten Godfrey "The YAMR: Yet Another Multipath Routing Protocol".*
6. *Giridhar Jayavelu, Srinivasan Ramasubramanian, "Maintaining Colored Trees for Disjoint Multipath Routing Under Node Failures," IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 17, NO. 1, FEBRUARY 2009.*
7. *Sumet Prabhavat, , Hiroki Nishiyama , Nirwan Ansari and Nei Kato, "On Load Distribution over Multipath Networks" IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 14, NO. 3, THIRD QUARTER 2012*