ISSN 2395-1621

Service Level Agreement Based IP Failure Handling By Localized On Demand Link State Routing

Angha Besake [#1], Pritee Bhanwase [#2], Geeta Pol [#3], Rohini Vanjari [#4]

[1]anghabesake@gmail.com
[2]priteebhnwase@gmail.com
[3]geetapol@gmail.com
[4] rohinivanjari@gmail.com

[#1234] Navsahydri College of Engineering.
Pune, Maharashtra, India.

ABSTRACT

IP failures commonly are observed in the network and there are several systems introduced to reroute packet which help to reach the destination. There are various systems available to handle the IP failures. These systems work properly in case of single failure, but they cause an error when it handles the multiple failures. To avoid this situation we provide a guarantee of forwarding a packet to its destination by using Localized on Demand Link State (LOLS) routing. In LOLS packet carries blacklist which consists of minimum set of unavailable links. When packet move towards its destination at that time blacklist can be reset. The next node is selected which has minimum weight. In this paper we provide the guarantee to forward the packet to its all reachable destination, in case of multiple failures. LOLS requires 6 bits to forward the blacklist information.

Keywords— Localized On Demand Link State (LOLS),Local Rerouting, Fast Rerouting, Failure Resilience, Blacklist..

ARTICLE INFO

Article History

Received : 20th April 2015

Received in revised form :

22nd April 2015

Accepted :26th April 2015

Published online : 22nd May 2015

I. INTRODUCTION

The internet is widely used for critical application in the network which is expected always available. Unfortunately, even in well managed network service disruption occurred due to node failures. There are various studies observed on frequency[7]-[5], type and failed links in IP network. Many of the failures are reported common and widely transient. Less than a minute 46% reported and less than ten minute 86% reported. For supporting to upcoming sensitive application in day to day internet, these systems need to work effectively with miner disruption. For example the interruption time of longer than 50 ms is ignored for critical application[4]. For this there is main challenge for service provider to provide the uninterrupted service. While many failures are found in single failure at one study it found up to 30% of failures[6] .Due to service interruption causes multiple failures in the network. Therefore it is necessary to develop a such system which help to resolve the multiple failures as well as single failures. Our work is to fulfill the network requirement.

The various link state routing protocol such as OSPF and ISIS these are design to route around the failed links but needed the high availability[7]. Multi-protocol Label switching [8]it work on the label techniques so it can handle the temporary failure. However it is not useful for the backup label path. There are several rerouting protocols which handle the failures in the network without notifying the whole network about failure link[9][10]. These systems are design to handle single or correlated failures[1]. Packet recycles (PR)[3] and failures carrying packet (FCP)[2] both are send the packet to destination, in case of arbitrary number of failures. The main disadvantages of FCP it carries the failure information of node to destination.

II. RELATED WORK

The failure in the network needs to be handled for which various approaches have been proposed in past various different working fragments are included in these approaches of networking and these are various other components which are to be focused on this schema . Few of these approaches are described below of this work field.

Single and Correlated failures:

By using MRC, the technique is used for the correction of the single and related failures. In MRC, for fast rerouting the adjacent nodes are checked at each level. Efficient performance for time constraints is given by FIFR[6]. This schema only recovers single failures but not multiple failures.

Multiple Independent Failures:

FCP was introduced after localized on demand link state routing. The drawback of the FCP was it carries the unnecessary information about the failed links all the way towards the destination which was undesirable .Packet recycle is a technique which used for rerouting this reduces the number of bits which is included in the packet header. The advantage of packet recycling is done by which the help of cellular graph embedding when even any packet is dropped in case of failure. But PR takes longer distance than LOLS.

Geographic Position Based Routing:

When the packet is close to the destination the forwarding of the packet is changed to the face mode. With the help of planarized sub graph boundaries the packet is moved in the face mode for sub optimal path the topology based routing does not provide high scalability than position based routing.

Localized Link State Update:

The limited dissemination was introduced with the purpose of providing scalable routing of mobile ad-hoc networking in link list state routing. We can update the nearest node at a high frequency than the remote node outside a given scope with the help of Fisheye State Routing and Hazy Sighted Link State Routing. A form of limited dissemination based routing schema that check loop free forwarding in the chance of failures which includes LOLS.

III. PROPOSED SYSTEM

LOLS provides protection against multiple failures[18]. When the current state is worse than the globally advertised state by LOLS the link is considered as degraded. In LOLS packet carries blacklist which consists of minimum set of unavailable links and excluding those links packet is forwarded to the next hop. When packet blacklist is initially empty and remains empty then there is no difference between the current and advertised state of link along its path. When packet arrives at a node with a degraded adjacent link to its next hop then this link is added to the blacklist

III. MOTIVATION

The earlier system the technique to handle loss of data, delayed timing, loss of acknowledgement was proposed but it did not describe how to redirect packet in, when the path is unavailable or corrupted. The system describes the content of multipath routing from the source to root destination within the network. It is mostly important handle single failure as well as multiple failures.

Let us compare LOLS with earlier system: In earlier system in FCP the failure information is carried all the way to the destination which is undesirable. And in LOLS the update of failure links in the network is provided as the next hop proceed forward. In 2DMRC it provides recovering against link failure but has higher cost. LOLs has low cost as compared to 2DMRC.FSR & HSLS updates the nearby nodes that lie outside a certain scope in that drawbacks is choose scope can be more than sufficient in some case & less than necessary in other case resulting in needless updates or forwarding loops. LOLS consist of a limited destination based routing scheme that ensure loop free wording LOLS can decrease the blacklist size. Compared to packet recycling forwarding path are shorter with LOLS.

IV. METHODOLOGY

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

- Modules
  1.Server
  2.Client
  3.Router
  4.SLA Module.

Few details are as follows:

1. Client Module

In Module 1 we use the Java (Socket Programming) to create windows based GUI application which This module is used to send the data to server through routers and we use the MySql as Backend.

2. Server Module

In Module 2 we use the Java (Socket Programming) to Create windows Based GUI application which this module is used to receive the data send by the client

which came from the active router. It can have any number of clients and we use the MySql as Backend.

3. Routers Module

In Module 3 we use the Java to create windows Based GUI application. This module is used to placed in between server and client to transfer the data. Whenever client send the data to the server it will pass through any one router and we use the MySql as Backend.

4.SLA Module

In Module 4 we use the PHP(Hyper-text Preprocessor) to create a web based admin panel which can be used to This are placed in between server and client to transfer the data.Whenever client send the data to the server it will pass through any one router and we use the MySql as Backend.

1.Greedy Algorithm:

1.1 for each vertex v in V[G]
1.2 do define set S(v) ← {v}
1.3 Initialize priority queue Q that contains all edges of G,
1.4 using the weights as keys
1.5 A ← { } A will ultimately contains the edges of the MST
1.6 while A has less than n − 1 edges
1.7 do Let set S(v) contains v and S(u) contain u
1.8 if S(v) ≠ S(u)
1.9 then Add edge (u, v) to A
1.10 Merge S(v) and S(u) into one set i.e., union
1.11return A

In above greedy algorithm v is used for each vertex in graph. S(v) contain set of selected vertices which are choose to send packet. Queue is used for storing all edges and their weight. A is current available node for sending data which is checking Minimal Spanning tree. In queue contain at least one node that is starting node for sending data. Then A has less than n-1 edges. S(u) contain unvisited node/vertex. Then condition is checking S(v) is not equal to S(u). and add next edges(u,v) to A. Then total visited and unvisited node into one set e using union and return A.

2.Blacklist Algorithm

2.1 for each vertex v in V[G]
2.2 do define set S(v) ← {v}
2.3 Initialize priority queue Q that contains all edges of G, using the weights as keys
2.4 B ← { } B will ultimately contains the edges of the blacklist
2.5 while B has less than n − 1 edges
2.6 do Let set S(v) contains v and S(u) contain u
2.7 if S(v) = S(u)
2.8 then Add edge (u, v) to B
2.9 Merge S(v) and S(u) into one set i.e., union
2.10 return B

In above blacklist algorithm is apply every vertex because blacklist is updated every node in the network. v is used for each vertex in graph. S(v) contain set of selected vertices which are choose to send packet. Queue is used for storing all edges and their weight. B is current available node for sending data. In queue contain at least one node that is starting node for sending data. Then B has less than n-1 edges. S(u) contain unvisited node/vertex. Then condition is checking S(v) is equal to S(u) then cycle is generated and add next edges(u,v) to Blacklist. Then total visited and unvisited node into one set e using union and return B.

3.Backtracking Algorithm

3.1 Define stack as S(B)
3.2 For each S(B) as s
{
3.3 B= pop(s)
3.4 A = Greedy(B)
3.5 If(A)
{
3.6 Break;
}
3.7 End for each

In backtracking algorithm we are using stack for storing vertex. Backtracking can also apply each vertex. S(B) is set of backtracking vertex. Suppose stack contain A,B,C we can pop stack vertex if path is not available then selecting previous vertex which have available path to send data. After selecting A then break the pop condition A is sending data towards destination.

System Architecture:

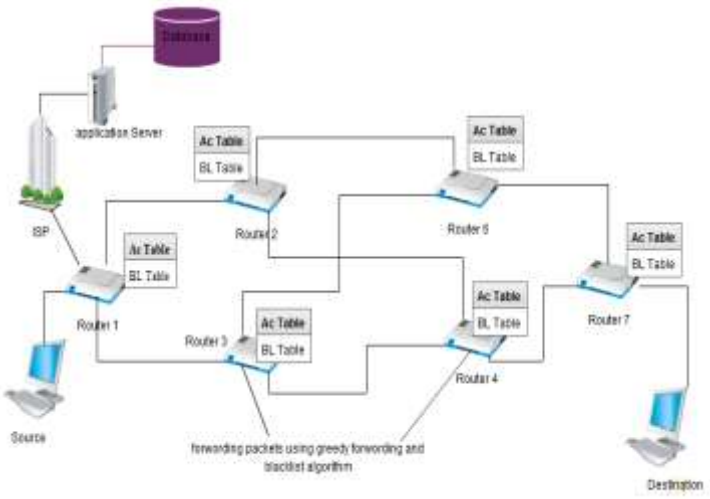


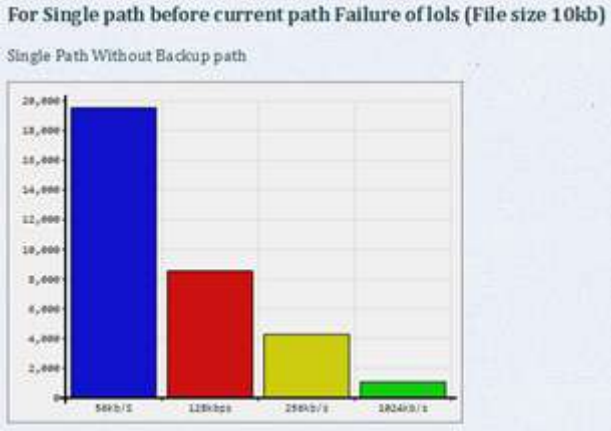
Fig 1. System Architecture

In above fig System architecture consist database which include in application server. That application server also include in ISP(Internet Service Provider).ISP is a company that provides individual and other companies access to the internet and other related service such as website building and virtual hosting. The information of failed link from every router in the network which is consist in database. In network when sending packet from source to destination the each packet contain blacklist and acceptance table. Blacklist

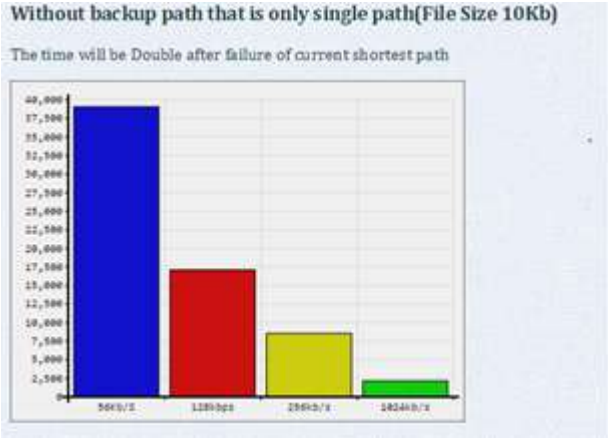
contains failed link information and acceptance table contain selected node to forward packet which path are available. Blacklist and acceptance table get updated to every node and forwarding packet to available path. This process is continue until packet reaches to its destination.

VI. EXPERIMENTAL RESULT AN ANALYSIS

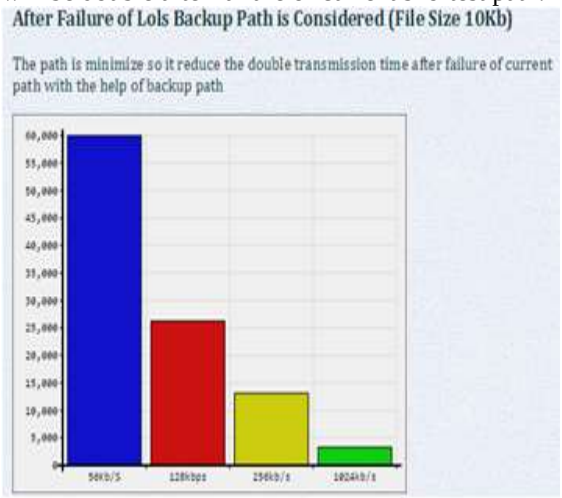
17.4386 Msecond with 56kb/s speed and 610.352 Mseconds with 128kbs and 305.176 Mseconds with 256kb/s and 76.2939 Mseconds with 1024 kbps speed hence kb file will be transfer upto 1m in174.386 msecond with 56kb/s.



In the first graph shows the single path before current path failure of LOLS(Localised On Demand Link State) Routing.In the first graph Consider single path when the tranfering packet from sorce to destination.



In the second graph shows without backup path that is only single path. In the second graph the packet transfer source to destination in that consider only shortest path which is not failures on time . So when the packet send using shortest path and on failure occurrence then retransmission is done but its taking double time to finish another shortest path in the network. The time will be double after failure of current shortest path.



Third graph show the after failure of localized On demand Link State routing (LOLS) Backup path is consider. In this graph consider the backup path when the shortest path is fail on time when packet send source to destination in that when shortest path is fail the using another minimum shortest path (backup path) in the network choose to send the packet. Using backup path we are saving the time for the transmission. The path minimize so it reduce the double transmission time after failure of current path with the help of backup path.

Graph Conclusion

For Single path before current path failure of localized on demand link state routing. The time required is (256kb/s):39062.52MSecond. For single path after current path failure of lols. The time required is (256kb/s): 59988.87MSecond. Hence save (39062.52-59988.87): 20926.35

VII. Conclusion And future work

a In this paper we describe how to handle multiple failures using LOLS. The basic idea behind LOLs, the packet carries blacklist and the acceptance table. In blacklist we have failed link and acceptance table contain available path .LOLS has a feature of updating the blacklist as soon as it takes the next hop. Inspiteof multiple failures LOLS assure loop-free forwarding towards destination. Without any LOLS we provide service to customer using SLA. While sending the packet in the network if on-time failure occurs for the chosen shortest path then the packet will choose another shortest path i.e backup path. Hence, we can reduce the transmission time for sending packet in the network. We have successfully implemented LOLS for wide area network. The future scope of our project is handle physical failure

REFRENCES

[1] A . Besake, P. Bhanwase, G . Pol, and R . Vanjari," Service Level Agreement Based IP Failure By Using Localized On Demand Link State Routing," *Networking*, Volume 1, Issue 4, October -2014.

[2] Glenn Robertson And Srihari Nelakuditi.," Handling Multiple Failures In Ip Networks Through Localized On-Demand Link State Routing" Ieee Transactions On Network And Service Management, VOL. 9, NO. 3, SEPTEMBER 2012.

[3] S. Kini, S. Ramasubramanian, A. Kvalbein, and A. Hansen, "Fast recovery from dual link or single node failures in IP networks using tunneling," *IEEE/ACM Trans. Networking*, vol. 18, no. 6, pp. 1988–1999, Dec. 2010.

[4] S. S. Lor, R. Landa, and M. Rio, "Packet re-cycling: eliminating packet losses due to network failures," in *Proc. 2010 HotNets.*

[5] P. Francois and O. Bonaventure, "Avoiding transient loops during IGP convergence in IP networks," *ACM Trans. Networking*, vol. 15, no. 6, pp. 1280–1292, Dec. 2007.

[6] O. B. et al, "Achieving sub-50 milliseconds recovery upon BGP peering link failures," in *Proc. 2005 CoNEXT*

[7] A. Gonzalez and B. Helvik, "Analysis of failures characteristics in the uninett IP backbone network," in *Proc. 2011 IEEE Workshopsof International Conference on Advanced Information Networking andApplications*, pp. 198–203.

[8] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.-N. Chuah, Y. Ganjali, and C. Diot, "Characterization of failures in an operational IP backbone network," *IEEE/ACM Trans.Netw.*, vol. 16, no. 4, pp. 749–762, Aug. 2008. Available: http://dx.doi.org/10.1109/TNET.2007.902727

[9] G. I. *et al.*, "Analysis of link failures in an IP backbone," in *Proc. 2002 ACM IMW.*

[10] A. K. *et al.*, "Fast IP network recovery using multiple routing configurations,"in *Proc. 2006 IEEE Infocom.*

