International Journal of Advanced Engineering & Innovative Technology (IJAEIT)
Volume 1, Issue 4, October -2014
ISRA IMPACT FACTOR: 0.42

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

Angha Besake, Pritee Bhanwase, Geeta Pol,Rohini Vanjari

ABSTRACT — There are several proposed system for carrying single failure based on local rerouting which provides high network availability despite failures. Most of the above proposed systems are effective in handling single failures, but they cause loops or dropping of packets, delayed timing in case of multiple independent failures. We ensure forwarding of packet to its reachable destination with help of Localized on Demand Link State (LOLS) routing. In LOLS, every packet carries blacklist along with it which consists of minimal set of failed links towards its destination next node will be decided by excluding those failed links. The blacklist is updated as soon as packet takes next hop, this process is continued until the packet reaches its destination which can be encoded in few bits. In this paper we describe to ensure forwarding of packet to all reachable destination in case of multiple failures. In worst case, LOLS needs 6 bits convey the blacklist information.

Index Term- Fast Reroute, Failure Resilience, Local Rerouting, LOLS.

1 INTRODUCTION

The Internet is expected to be always available and is used for mission critical application. In spite of well managed networks service disruptions occurs due to link and node failures. In IP backbone network there have been some studies [1-2] about duration, frequency and type of failures. Most of the failures are transient and fairly common: 86% of failures last less than ten minutes and 46% of failures last than a minute. Using minimal service disruption the networks need to survive failures for supporting emerging time-sensitive application in today's Internet. For example, In mission critical application a disruption time longer than 50 ms is considered intolerable [3]. A major challenge for service providers is providing uninterrupted service availability despite transient failures.

Most of the failures are observe to be single failures, but [4] approximately 30% of unplanned failures that involve multiple links, which is significant fraction. Multiple failures can be cause of service disruption which is quite significant. Hence it has become necessary to invent schemes which will protect network against single failure as well as multiple independent failures. Our work focuses on some of the recently propose routing scheme and is motivated by this need. OSPF and ISIS are link state routing protocols which are designed to route around in spite failed links but for supporting high availability they lack the resilience [1]. Multi-protocol Label Switching [8] it is label based technique so that it can handle transient failures effectively. It is not scalable to configure many backup label switched paths so it does not provide security against multiple independent failures. MPLS based recovery scalable to multiple failures was attempted by authors but assumption was made on past statistics, probable failure pattern on the network failures are called as MPLS control plane.

In IP network there have been several reroute proposals for handling failures it has adjacent node which perform local rerouting without notifying about failure in the network [5-6]. However these schemes are design to handle single or co related failures only. Recently [7] proposed system can handle dual link but no single link fail. In case of arbitrary number of failures the failures carrying packet (FCP) [8] and packet recycle (PR) [9] try to forward packets to the reachable destination. The drawback of FCP is that is carries failures information in each packet all the way to the destination and PR forward the packets along long distance.

- *Angha Besake, Pritee Bhanwase, Geeta Pol,Rohini Vanjaris currently in department of Computer engineering in. Department of Computer Engineering ,Navsahyadri Education Society's Group of Institutions, University of Pune, Naigaon, Pune 412213 India*

2 RELATED WORK:

There have been various proposed approaches made in past to handle the failures into the network. These approaches include various different working fragments into networking there are many other components which

are to be focused on this schema. Following we describe some approaches into this work field.

3 SINGLE OR CORRELATED FAILURE:

This technique is used for correction of single and correlated failure by using MRC. At each level it checks adjacent node and link to make faster rerouting. Failure Inferencing Based Fast Rerouting (FIFR) [10] gives efficient performance for time constraints. This schema is used for recovering single failures but not multiple failures.

4 MULTIPLE INDEPENDENT FAILURES:

FCP was introduced after Localized On-Demand Link State Routing.FCP carries the unnecessary information of the failed links throughout its journey towards destination which is not suitable. Packet Recycling is a technique for successful rerouting it reduces the number of bits which is included in the packet header. The advantage of packet recycling, whenever any packet drops in a case of failures then reroute the packet by using cellular graph embeddings.PR takes longer distance than LOLS.

Geographic Position Based Routing:

The forwarding of the packet is changed to the face mode when the packet is close to the destination. In face mode packet is moved along with the planarized subgraph boundaries. Topology based routing does not provide high scalability than position based routing for sub optimal path.

5 LOCALIZED LINK STATE UPDATE:

The purpose behind introducing limited dissemination is providing scalable routing for mobile ad-hoc networking in link state routing. Using Fisheye State Routing (FSR) and Hazy Sighted Link State Routing we can update closest node at a great frequency than the remote node lying outside certain scope. Localized On Demand Link State Routing can be included as a form of limited dissemination based routing schema that check loop free forwarding in the chance of failures.

6 PROPOSED METHODOLOGY:

The protection again multiple failures is done by Localized On-demand Link State (LOLS) Routing[18].The link are considered as degraded if its current state is worst than globally advertise by LOLS. In LOLS packet send in the network carries blacklist along with it that is a minimal set of degraded link encounter along its path and the next hop of packet is decided by excluded blacklisted links. There is no difference between the current and advertised state of link along its path when packet blacklist is initially empty and remains empty. The link is added to the blacklist when packets arrives at a node with a degraded adjacent link to its next hop.

7 SYSTEM ARCHITECTURE:

Now consider the following diagram to know about the system architecture. The system architecture has ISP (Internet Service Provider).ISP is an organization that provides Service for accessing, using and participating in the internet. ISP contains the application server, the database is stored in an application server. The database consists of the failed links from every router in the network. While sending the packet from source to the destination the packet will carry a blacklist and acceptance list along with it. The packet will check the blacklist and decide its next hop excluding the failed links in the blacklist. As soon as the packet takes next hop the blacklist will get updated which will consists of failed link from at particular router again the same procedure will be repeated and finally the packet will reach to its destination.

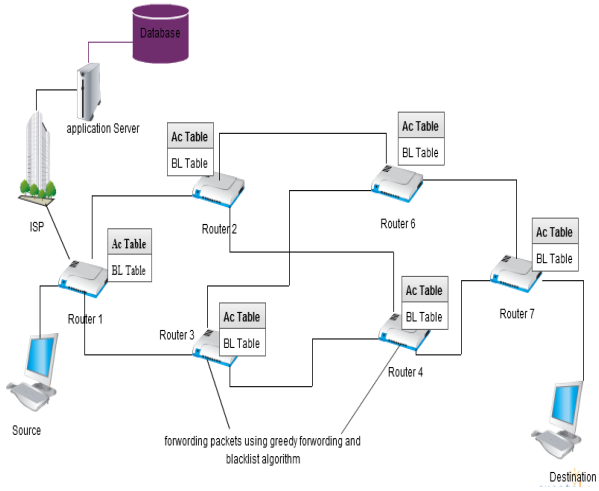

Fig1.SystemArchitecture

I] Algorithm:

1. Check for nodes.
2. If node found apply greedy forward and backward algorithm.
2.1 Check nearest node.
2.2 If nearest node found transfer data to that node.
2.3 If node is failure then add node to the blacklist.
2.4 Check for another path.
2.5 If path found then transfer data.
2.6 If node is Dead end then backward data to previous node.
2.7 Go to step 1 again.
3. Store blacklist in database.
4. Transfered packet through available path.
5. Receive packet at destination.

II] Mathematical Model:

1] U is main set of users like u1, u2, u3….
U = {u1, u2, u3…….}
2] A is main set of Administrators like a1, a2, a3….
A = {a1, a2, a3…….}
3] R is a set of routers like R1,R2,R3…
R= {R1, R2, R3……..}
4] R1 is a set of participating path P1,P2,P3….
R1= {P1, P2, P3……..}
5] P1 is a set of process p1,p2,p3….
P1= {p1, p2, p3……...}
6] p1 is a set of subprocess e1, e2, e3, e4, e5
p1= {e1,e2,e3,e4,e5}
Where
{e1=Find the nodes in the network}
{e2=Provide the weights to the each links in the network}
{e3=Perform Greedy forwarding and Backwarding algorithm}
{e4= Generate blacklist for each packet and apply blacklist based forwarding algorithm}
{e5= Integrate system with LOLS}

8 CONCLUSION AND FUTURE SCOPE:

In this paper we represent LOLS,Localized On Demand Link State Routing to handle multiple failure in IP network.In order to ensure the loop free forwarding LOLS carry packet along with blacklist consisting failed links along its path. LOLS provide a feature that the packet blacklist is updated when it moves towards the destination. LOLS provide a guarantees for loop-free forwarding to destination inspite of multiple failures in the network. Using a SLA(Service Level Agreement) we provide service to the customer, and ensures forwarding of the packet to destination with any loss. Our plan is to implement LOLS for wide area network. Our future scope is to handle physical problem in the network.

9 REFERENCES:

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

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

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

[4] 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

[5] S. Bryant, M. Shand, and S. Previdi, "IP fast reroute using notvia addresses," Internet Draft(work in progress), Mar. 2006, draftbryantshand-IPFRR-notvia-addresses-02.txt.

[6] S. Rai, B. Mukherjee, and O. Deshpande, "IP resilience within an autonomous system: current approaches, challenges, and future directions,"*IEEE Commun. Mag.*, pp. 142–149, Oct. 2005

[7] 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.

[8] K. Lakshminarayanan, M. Caesar, M. Rangan, T. Anderson, S. Shenker, and I. Stoica, "Achieving convergence-free routing using failure-carrying packets," in *Proc. 2007 SIGCOMM*, pp. 241–252.

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

[10] V. Sharma and F. Hellstrand, "Framework for MPLS-based recovery,"RFC 3469, Feb.2003.

.