International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 1, January - 2014

A Localized on-Demand Link State Routing for Handling Multiple Failures in IP Networks.

Prof. S. M. Sangve
Comp dept.
ZES's Dnyanganga College of Engineering and research.
Pune, Maharashtra ,India.

Pratap Patil
Comp dept.
ZES's Dnyanganga College of Engineering and research Pune, Maharashtra ,India.

Kunal Solanke
Comp dept.
ZES's Dnyanganga College of Engineering and research.
Pune, Maharashtra ,India.

Sushil Warkar
Comp dept.
ZES's Dnyanganga College of Engineering and research.
Pune, Maharashtra ,India.

Amit Shirke
Comp dept.
ZES's Dnyanganga College of Engineering and research.
Pune, Maharashtra ,India.

Abstract: We observe that there is failure in an IP network and these failures are common which may creat an obstacle. A localized on demand link state routing is used in such a case to make the failure chances negligible. We here use Greedy Forwarding and Blacklist based forwarding algorithm for handling such a failure within our IP network. Greedy based uses a weight based distribution which find out efficient path and then work along with the blacklist to get most efficient path during packet forwarding. LOLS i.e. localized on demand link state routing make it to work on multiple failures thus we can handle multiple failures within a network. This paper elaborates how it implements to assure forwarding to all reachable destinations in case of any two link failure. LOLS, each packet has a *blacklist*, which has a set of failed links along its path, and the next hop is determined by eliminating the blacklisted links. We also used Multiple Routing Configuration Protocol in a purpose for faster re-routing and thus it works more efficiently into a network. The evaluation of such failure scenario dependent on various real network topologies that reveals LOLS requires 6 bits in the worst case to convey the blacklisted information. We argue that the overhead is acceptable considering the LOLS routing deviates from the optimal path.

Index terms: Failure Resilience, Fast Rerouting, Optimal Path, Packet Forwarding.

INTRODUCTION:

Now a day there is rapid use of internet and a small disturbance in a network that may be due to any reason causes a greater trouble in work although it might be of few microseconds. Internet being prior in day to day life has become an integral part and avoiding its connectivity hindrances is another major part thus the failure might be due to link or node. So we have tried to make an efficient and effective way to handle such a failure using Localized on demand link state routing protocol. Here in our implementation we check for a demand at the last end and then proceed by the request of the demand thus our distribution becomes much more efficient that is how we work in LOLS[1]

Here faster re-rerouting[7] in case of link failure is also an prior part because we have to ensure quicker recovery in case of link failure and which is our main aim. We have OSPF and MRC which ensures faster re-routing at any stage of our consideration and that is why we have implemented MRC[2] i.e.OSPF is not preconfigured into our system it is needed to be made and brought to be made available into our system for the purpose of its working. We have MRC preconfigured and also checks for various availabilities it also checks for the loss into packets as well as is an connectionless approach thus it make our system more convenient and reliable for faster rerouting. We also have IGP and BGP for faster rerouting but they are less convenient than that of the MRC as they take a much more time to choose the adjacent node through which the data transfer is going to actually occur and thus becomes a bit time consuming than that of the MRC[4][2].

Here MRC[2] provide various features like connectionless,gurantted, biconnect,node fault,link fault and many other attributes so it is more useful in faster rerouting.

Greedy Forwarding: We have referred to Greedy forwarding algorithm which also makes us to detect a failure into an node it checks for sink node and sensor node[3]. The sink node which is more convenient is being used and the data is sent to the sensor node thus both of them work into progression and by this they show efficient and convenient data transfer the sink node check out for next sink node and by using sensor node transfer and manipulate the link or the node failure[3][8].

The greedy forwarding check out for each node and the nearby node during its transfer in case or link and node failure.Each sink node is maded upto the mark for the purpose to send it to other sensor node and thus it can be used to recover from the failure which may occur into an IP network due to noisy channel or other network problem it uses wireless transmission scheme for such a purpose. So here greedy forwarding checks for weight at each node or link and accordingly check for its appropriate minimal set of path for forwarding packet. Here in those case we have used bandwidth as a part of the weight into our system and thus we only check out for the bandwidth and its weight at this condition of greedy forwarding algorithm[8].

Blacklist Aided Forwarding: The next algorithm which we have used into our system is Blacklist Aided Forwarding[4] (BAF) also called as Blacklist Forwarding Algorithm. It checkout for the packet which are being blacklisted and thus use these blacklisted link and forward the packets. It is much more useable and reliable as well as it is most efficient method for the forwarding of the packet in case of link or the node failure as it checks for each and every level and it makes the connection by listing out how many times the node failure has exactly occurred. This information provided using blacklist based forwarding is used in order to get the node and link failure into our network and ensures how the forwarding exactly takes place. The blacklist table is maintained by the packet header which enables it to check whether the forwarding should be done or not.

By using the Blacklist Aided Forwarding we can checkout for the the link which has maximum chances of failure and avoid transfer of the packet using such a link . Thus minimize the chances of node or the link failure by using Blacklist forwarding algorithm[4].The blacklisted link is avoided and the probability of the link failure is obtained in this algorithm and thus we can find out whether the link is good enough to forward the packet at the given condition and thus we can ensure the node and link failure doesn't occur at that particular stages or the phases. Thus Blacklist Aided Forwarding along with Greedy Forwarding both together work parallelly in order to make a complete detection and recovery of link failure and thus make our system more convenient and much more scalable as well as make it good and worthy enough for faster rerouting in order to avoid time constraint. The time required to reroute and recover the link is reduced a result of use of the Blacklist Aided Forwarding and Greedy Forwarding Algorithm and hence we can say it leads to achievement in faster rerouting and easy packet forwarding in case of link failure[15] .

Multiple Routing Configuration (MRC): Here MRC[5] provide various features like connectionless,gurantted biconnect,node fault,link fault and many other attributes so it is more useful in faster rerouting[13]. Here faster re-rerouting in case of link failure is also an prior part because we have to ensure quicker recovery in case of link failure and which is our main aim. We also have IGP and BGP for faster rerouting but they are less convenient than that of the MRC as they take a much more time to choose the adjacent node through which the data transfer is going to actually occur and thus becomes a bit time consuming than that of the MRC[15] . We have MRC preconfigured and also checks for various avabilities it also checks for the loss into packets as well as is an connectionless approach thus it make our system more convenient and reliable for faster rereouting.

RELATED WORK:

Many attempts are being made for the purpose of making a efficient way to handel the failure into the network. It include a variety of working fragments into this area but it has various other component that must be taken care of while working onto these scheme.Here we have show some of such a scheme into this work field

Single or Correlated Failures:
This phenomenon uses a single way routing using MRC[5] .It uses MRC for the purpose of single as well as correlated failure correction. It checks for adjacent node and link at each level and then makes faster rerouting moves at each phase. Failure Inferencing based Fast Rerouting (FIFR)[6] makes it

better for time constraints .The above given and other such a similar schemes
offer resilience against single failures but are not implemented to recover from multiple unrelated and unfamiliar failures

Geographic Position based Routing:

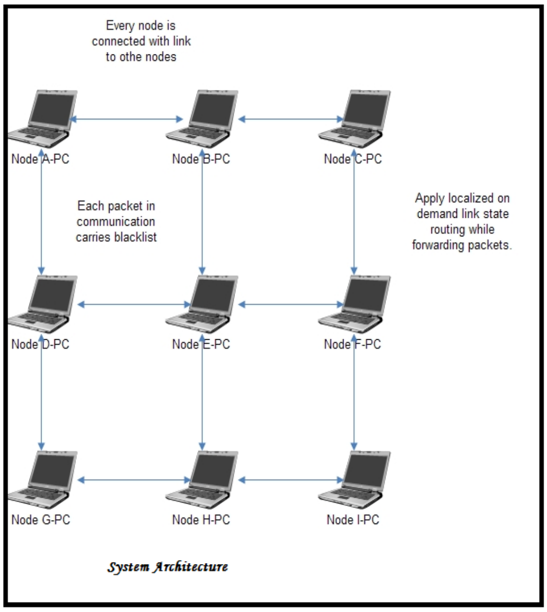
It is much more similar to that of greedy mode[3]. When the *dead-end* is reached by packet i.e., when the destination is closer to forwarding node than any of its adjacent nodes, then the forwarding is changed to *face* mode. The packet switched to greedy mode when it reaches to the destination.

Localized Link State Updates:

The limited dissemination dependent schemes have been proposed to make link state routing more scalable for mobile ad-hoc networks. Fisheye state routing[1]-[6] (FSR) schemes upgrades the given nearby nodes at a larger frequency than the remote nodes which lie outside a certain scope. Localized On demand Link State can be considered a form of limited dissemination based routing scheme that check out for loop-free forwarding while giving an notification only a small subset of nodes in the chance of a failure.

System Architecture:-

Now consider the below diagram to know about system architecture in detail, here we have a source node A and Destination I. At node A we check for shortest path which is B but B is blacklisted so we move to node D then We check for the node E and G. E is the shortest and has no blacklisted link so is reliable to transfer packet so we choose node E.



After the reach node E we have two adjacent nodes F and H. here the shortest path is at node F so we traverse along path F then again we have two adjacent nodes to F i.e. I and C. but I has minimum Weight as well as it is our destination node so we move across node I.thus we reach from source to destination more reliably and fastly. This is how the system works.

Conclusion:

In this paper, we have represented LOLS, a localized on-demand link state routing for the purpose of handling and recovering multiple IP failures in networks. The main idea for LOLS is to have packets carry a blacklist of degraded links enraptured along the path that are to be neglected in order to make sure loop-free forwarding. The main feature of LOLS is that a packet's are blacklist is reset as earlier it makes forward progression to the destination, and then limiting the failure information to just a few hops. Hence we have proved that a Localized on-demand link state routing ensures loop-free forwarding to required destinations without taking into account the number of failures in the network. We have enhanced the overhead due to Localized On-demand Link State using large real-time topologies and shown that it scales even more better than the recently proposed scheme failure carrying packets which has much more similar failure resilience objectives. We have also shown a practical version of a Localized On-demand link state for the protection against declared failures, and shown that it needs only a noblest number of header bits or not-through addresses for handling any two link or node failures. The aim is to implement a prototype of Localized On-demand Link State using a Mininet system to show a demonstration of its deplorability.

REFERENCES:

[1] 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.

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

[3] B. Karp and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in *Proc. 2000 ACM Mobicom*, pp. 243–254. Available: citeseer.ist.psu.edu/karp00gpsr.html

[4] S. N. et al, "Blacklist-aided forwarding in static multihop wireless networks," in *2005 SECON*.

[5] A. Kvalbein, T. Cicic, and S. Gjessing, "Post-failure routing performance with multiple routing configurations," in *2007 IEEE INFOCOM*.

[6] G. Robertson, J. Bedenbaugh, and S. Nelakuditi, "Fast convergence with fast reroute in IP networks," in *2010 IEEE HPSR*.

[7] S. Bryant, M. Shand, and S. Previdi, "IP fast reroute using not-via addresses," Internet Draft (work in progress), July 2007, draft-ietf-rtgwgipfrr- notvia-addresses-01.txt.

[8] A. Li, X. Yang, and D. Wetherall, "SafeGuard: safe forwarding duringrouting changes," in *2009 CoNEXT*.

[9] M. Gerla, X. Hong, and G. Pei, "Fisheye state routing protocol for ad hoc networks," IETF Internet Draft, June 2002, draft-ietf-manet-fsr-03.txt.

[10] M. Shand and S. Bryant, "IP fast reroute framework," RFC 5714, January 2010.

[11] S. Nelakuditi et al., "Failure insensitive routing for ensuring service availability," in IWQoS'03 Lecture Notes in Computer Science 2707, Jun. 2003.

[12] A. Kvalbein, A. F. Hansen, T. Cicic, S. Gjessing, and O. Lysne. Fast IP network recovery using multiple routing configurations. In *IEEE INFOCOM*, 2006.

[13] K. Lakshminarayanan, M. Caesar, M. Rangan, T. Anderson, S. Shenker, and I. Stoica. Achieving convergence free routing using failure-carrying packets. In *ACM SIGCOMM*, 2007.

[14] H. A. B. F. Oliveira, A. Boukerche, E. F. Nakamura, and A. A. Loureiro, "Localization in time and space for wireless sensor networks: An efficient and lightweight algorithm." *Performance Evaluation*, vol. 66, no. 3-5, pp. 209–222, 2009.

[15] K. Langendoen and N. Reijers, "Distributed localization in wireless sensor networks: a quantitative comparison," vol. 43, no. 4. New York, NY, USA: Elsevier North-Holland, Inc., 2003, pp. 499–518.