ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A Mechanism to Overcome Link Failures in Single Path Network Architecture

Asma Parveen[*1], Dr. Mohammed Abdul Waheed[2]
[*1] Research scholar, JJT University, Jhunjhunu, Rajasthan, India
[2]Associate Professor, VTU Regional office, Gulbarga, Karnataka, India
profasma.cse@gmail.com

Abstract

In a single link network architecture if a link fails, system hunts for the substitute link and transmits the data through that link. It is always necessary for system to search the reason for path break then configure the system again to transmit the data through other path/node. But during the transmission there are more chances of packet loss or delay. In this paper we propose a mechanism to overcome from the packet loss or delay problem such that if any node or path breakdowns, it will assist in transmission of data without any packet loss or delay.

Keywords: Node and Link Failures, Packet loss, delay, retransmission, OSPF

Introduction

Failures in high-speed networks have always been a concern of utmost importance. At present link failures are pretty common in the networks environment. Normally if one link gets fail in single link network architecture, system hunts for the substitute link and send out the data through that link. In this situation it is essential for system to find out the root cause for its path failure after that configure the system for a second time to send out the data through another node or path. At the time of transmission more chances are there for packet loss or delay.

To overcome from this packet loss or delay problem we propose a new approach. In this approach, even if any node or path breakdowns, it will assist in transmission of data without any packet loss. Always it will maintain substitute path in buffer. As the primary path is failed, it will automatically connect to substitute path which is considered as second shortest path from source to destination. If a breakdown happens in node or path, it will pop up the notification to the users and will go for the second shortest path for transmitting the data [15].

This paper will study problems of network path and node failures and propose a mechanism which can assist in smooth transmission of data in networks without packet loss or delay.

The procedure is planned for the recovery in TCP/IP network because of the connection and node breakdown. It is capable to recuperate connection and node breakdowns in IP networks very fast which is deliberate in milliseconds. It employs a minor set of alternate path for routing setup. That endorsement helps to desire another path presented in routing table after the breakdown in the poles apart of the system, the backup configurations link weights are set to stay away from routing traffic. Network superintendent monitor that all links which are combined to number of systems are provided adequately high connection weights or not. The breakdown of the network system will be able only to influence network traffics that is started at or destined for the system itself. To prohibit a connection or a multiple groups of connections from it involves the routing, an infinite load is assigned to it and then that link can be not making the grade with no cost for the traffic [16].

Related Work

Much work has lately been done to improve robustness against component failures in IP networks. In this section, we focus on the most important contributions aimed at restoring connectivity without a global re-convergence. This summarizes important features of the different approaches. We indicate whether each mechanism guarantees one-fault tolerance in an arbitrary bi-connected network, for link and node failures, independent of the root cause of failure (failure agnostic). We also indicate whether they solve the “last hop problem”. Network layer recovery in the timescale of milliseconds has traditionally only been available for networks using MPLS(multi-protocol label switching) with its fast reroute extensions. In the discussion below, we focus

mainly on solutions for connectionless destination-based IP routing [5].

IETF has recently drafted a framework called IP fast reroute where they point at Loop-Free Alternates (LFAs) as a technique to partly solve IP fast reroute. From a node detecting a failure, a next hop is defined as an LFA if this next hop will not loop the packets back to the detecting node or to the failure. Since LFAs do not provide full coverage, IETF is also drafting a tunneling approach based on so called "Not-via" addresses to guarantee recovery from all single link and node failures. Not-via is the connectionless version of MPLS fast re-routing where packets are detoured around the failure to the next-next hop [6]. To protect against the failure of a component P, a special Not-via address is created for this component at each of P's neighbors. Forwarding tables are then calculated for these addresses without using the protected component. This way, all nodes get a path to each of P's neighbors, without passing through ("Not-via") P. The Not-via approach is similar to this concept in that loop-free backup next-hops are found by doing shortest path calculations on a subset of the network. It also covers against link and node failures using the same mechanism, and is strictly pre-configured. However, the tunneling approach may give less optimal backup paths, and less flexibility with regards to post failure load balancing [7].

P. Narvaez et al. Propose a method relying on multi-hop repair paths. They propose to do a local re-convergence upon detection of a failure, i.e., notify and send updates only to the nodes necessary to avoid loops. A similar approach also considering dynamic traffic engineering is presented. We call these approaches *local rerouting*. They are designed only for link failures, and therefore avoid the problems of root cause of failure and the last hop. Their method does not guarantee one-fault-tolerance in arbitrary bi-connected networks. It is obviously connectionless. However, it is not strictly pre-configured, and can hence not recover traffic in the same short time-scale as a strictly pre-configured scheme [12].

Nelakuditi *et al.* propose using interface specific forwarding to provide loop-free backup next hops to recover from link failures. Their approach is called failure insensitive routing (FIR). The idea behind FIR is to let a router infer link failures based on the interface packets are coming from. When a link fails, the attached nodes locally reroute packets to the affected destinations, while all other nodes forward packets according to their pre-computed interface specific forwarding tables without being explicitly aware of the failure. In another paper, they have also proposed a similar method, named Failure Inferencing based Fast Rerouting (FIFR), for handling node failures. This method will also cover link failures, and hence it operates independent of the root cause of failure. However, their method will not guarantee this for the last hop, i.e., they do not solve the "last hop problem". FIFR guarantees one-fault-tolerance in any bi-connected network, it is connectionless, pre-configured and it does not affect the original failure-free routing [13][8].

Our main inspiration for using these functions to achieve failure recovery has been a layer-based approach used to obtain deadlock-free and fault-tolerant routing in irregular cluster networks based on a routing strategy called. General packet networks are not hampered by deadlock considerations necessary in interconnection networks, and hence we generalized the concept in a technology independent manner and named it Resilient Routing Layers. In the graph-theoretical context, RRL is based on calculating spanning sub topologies of the network, called layers. Each layer contains all nodes but only a subset of the links in the network [9].

None of the proactive recovery mechanisms discussed above takes any measures towards a good load distribution in the network in the period when traffic is routed on the recovery paths. Existing work on load distribution in connectionless IGP networks has either focused on the failure free case or on finding link weights that work well both in the normal case and when the routing protocol has converged after a single link failure.

Many of the approaches listed provide elegant and efficient solutions to fast network recovery, however Not-via tunneling seems to be the only two covering all evaluated requirements. However, we argue that this approach offers the same functionality with a simpler and more intuitive approach, and leaves more room for optimization with respect to load balancing.

Basically this paper is the reference from the IEEE base paper on Multi Path Configurations. As we got inspiration to work more on the research done through the concept of Multi Path Configurations, we present the concept of link failures.

It's always been a topic of interest to deal with the problems arises due to link or node failure on internet and provides solutions for revival from it. To be in such a big network like internet, the node or link breakdown discovery and its revival is quite time taking and lengthy process because it's generally subsequent to unsteadiness of the routing. While going through this lengthy procedure there could be the chances for packet drops. These situations is researched in BGP and IGP perspective, also it affects badly on live programs running on internet.

According to the base paper the concept allows recovery from all single link failures. Multi

Path Configurations concept was good to be taken as the base. As it only deals with the problem which arises with single link failure, it doesn't work for the situations where multiple links are broken. As this is the same case with most of the research works done for getting rid of single link failure situations, it also deals with the same [10].

To come up with the problems ignored by Multi Path Configurations and other researches, we provide solution in the form of our application concept which works on the cases where if alternative path is also broken then data would be transmitted through the third or the fourth path. Here we try to avoid the dependencies of the links on each other. This approach here is, prior to transmit information it searches for the paths available with minimum cost over the network. If the path is broken then it would take the second minimum cost path and if that path is broken then the third and so on [11].

Algorithms for protection against link failures have traditionally considered single-link failures for a detailed description on protection approaches. However, dual-link failures are becoming increasingly important due to two reasons. Firstly, links in the networks share resources such as conduits or ducts and the failure of such shared resources result in the failure of multiple links. Secondly, the average repair time for a failed link is in the order of a few hours to few days and this repair time is sufficiently long for a second failure to occur. Although algorithms developed for single-link failure resiliency is shown to cover a good percentage of dual-link failures, these cases often include links that are far away from each other. Considering the fact that these algorithms are not developed for dual-link failures, they may serve as an alternative to recover from independent dual-link failures. However, reliance on such approaches may not be preferable when the links close to one another in the network share resources, leading to correlated link failures [1].

A. Communication methods

To communicate our message from one machine to another, now-a-days there are number of methods which are known as communication methods are available, which can be defined as

- Electronic methods of communication: - Telephone
- Computerized methods of communication: - Internet

Now days with the popularity of internet, internet has become the most common method of communication as it provides the following facilities over the telephonic communication

- Cheapest method
- Fastest method

But due to the network setup breakdown the sluggish junction of routing code of behavior has been turn out to be serious issue which are growing very fast. Here the term Routing is possible specified as a practice of finding route or the next hop from source to destination for a packet. Routing is the function of network layer of the OSI model, a device which performs that function is known as routers. Routers use a table known as routing table to discover the direction of the packet's destination. The slab had all the details of the paths available which flow in form of packets from the source to destination and vice versa; router reads the header of each arriving packet and extracts its detonation address. After extracting the destination address router sends the packet on a best path, which is calculated by considering following points.

- Lowest cost
- Metric
- Hop count
- Congestion
- Load
- Bandwidth
- Latency
- Maximum transmission unit

B. Methods of Routing

There are two methods of routing

- Inert routing
- Active Routing

Inert routing:

It is a method of routing in which routing table are designed manually by the network administrator.

Active Routing:

Dynamic Routing is a method of routing in which routing table is maintained by the routing protocol. Some most common routing protocols are RIP, OSPF, DVP, and LSP. To conquer from this problem and for the fast recuperation from connection and node breakdowns in TCP/IP network setups, an innovative technology have been introduced which is known as Multiple Routing Configurations [14].

IP addressing and routing:

IP addressing entails the assignment of IP addresses and associated parameters to host interfaces. The address space is divided into networks and subnetworks, involving the designation of network or routing prefixes. IP routing is performed by all hosts, but most importantly by routers, which transport packets across network boundaries. Routers communicate with one another via specially designed routing protocols, either interior gateway

protocols or exterior gateway protocols, as needed for the topology of the network.

IP routing is also common in local networks. For example, many Ethernet switches support IP multicast operations. These switches use IP addresses and Internet Group Management Protocol to control multicast routing but use MAC addresses for the actual routing [17].

If we are making huge quantity of data transmission, it is indispensable to lessen the resource inaccessibility time because of breakdowns. Therefore, well organized and rapid revitalization methods from link and node breakdowns are made it compulsory in the development of rapid networks. Most of the algorithms which are implemented for security against breakdowns have typically made for single path/node breakdowns. The importance of link breakdowns is increasing more caused by two reasons. Primarily, in the shared networks systems if one among those is failed it cause for multiple links failure. Second, failure link normally it takes hours or some days to get it repair and this gap of repair time are cause for second link failure [2]. So it is indispensable to provide solutions for this problem. our new approach will resolves the path or node failures in the span of milliseconds. Even if any node or path breakdowns, it will assist in transmission of data without any packet loss.

In recent years the Internet has been transformed from a special purpose network to a ubiquitous platform for a wide range of everyday communication services. The demands on Internet reliability and availability have increased accordingly. A disruption of a link in central parts of a network has the potential to affect hundreds of thousands of phone conversations or TCP connections, with obvious adverse effects.

The ability to recover from failures has always been a central design goal in the Internet. IP networks are intrinsically robust, since IGP routing protocols like OSPF are designed to update the forwarding information based on the changed topology after a failure. This re-convergence assumes full distribution of the new link state to all routers in the network domain. When the new state information is distributed, each router individually calculates new valid routing tables.

This network-wide IP re-convergence is a time consuming process, and a link or node failure is typically followed by a period of routing instability. During this period, packets may be dropped due to invalid routes. This phenomenon has been studied in both IGP and BGP context, and has an adverse effect on real-time applications. Events leading to a re-convergence have been shown to occur frequently.

Much effort has been devoted to optimizing the different steps of the convergence of IP routing, i.e., detection, dissemination of information and shortest path calculation, but the convergence time is still too large for applications with real time demands. A key problem is that since most network failures are short lived, too rapid triggering of the re-convergence process can cause route flapping and increased network instability.

The IGP convergence process is slow because it is *reactive* and *global*. It reacts to a failure after it has happened, and it involves all the routers in the domain. In this paper we present a new scheme for handling link and node failures in IP networks. *The concept* is a *proactive* and *local* protection mechanism that allows recovery in the range of milliseconds. It allows packet forwarding to continue over preconfigured alternative next-hops immediately after the detection of the failure. Since no global re-routing is performed, fast failure detection mechanisms like fast hellos or hardware alerts can be used to trigger it without compromising network stability. This approach guarantees recovery from any single link or node failure, which constitutes a large majority of the failures experienced in a network It makes no assumptions with respect to the *root cause of failure*, e.g., whether the packet forwarding is disrupted due to a failed link or a failed router.

The shifting of traffic to links bypassing the failure can lead to congestion and packet loss in parts of the network. This limits the time that the proactive recovery scheme can be used to forward traffic before the global routing protocol is informed about the failure, and hence reduces the chance that a transient failure can be handled without a full global routing re-convergence. Ideally, a proactive recovery scheme should not only guarantee connectivity after a failure, but also do so in a manner that does not cause an unacceptable load distribution. This requirement has been noted as being one of the principal challenges for pre-calculated IP recovery schemes [3]. The link weights are set individually in each backup configuration. This gives great flexibility with respect to how the recovered traffic is routed. The backup configuration used after a failure is selected based on the failure instance, and thus we can choose link weights in the backup configurations that are well suited for only a subset of failure instances.

C. Existing System

Link failures in networks have negative effects on TCP links or telephonic conversation, with unfavorable impacts. The aptitude to pick up from breakdown is the key aim in the internet developments. IP networks are strong enough since OSPF are developed to revise the conveying information depended on the changed topology later

than a crash. This method consumes more time, and as time gone link or node stoppages may happen over and over again because of routing inconsistency. This situation may cause for packet loss because of void path [4].

Disadvantages:

1. There won't be any confidence that data reaches to the destination.
2. In the existing system there won't be any substitute path during single link failures.
3. It consumes more time.
4. Here we won't get clear cut information about failure paths.
5. A major drawback with existing systems is that they are vulnerable to packet loss or delay while data transmission during link failure.
6. User is not aware exactly where the path got broke.

Proposed System

In order to overcome from the drawback of the existing system, we propose a new approach in favour of managing a node or link stoppages in IP networks. Here we would use the approach that resolves the path or node failures in the span of milliseconds. Even if any node or path breakdowns, it will assist in transmission of data without any packet loss. Always it will maintain substitute path in buffer. As the primary path is failed, it will automatically connect to substitute path which is considered as second shortest path from source to destination. If a breakdown happens in node or path, it will pop up the notification to the users and will go for the second substitute path for transmitting the data.

Methodology

In this paper we propose to document all possible information related to path and node failures in network and propose a concept which can handle the problems arise due to link failures.

The concept here provides user with the option to choose the medium of transmission. If user chooses Serial approach then the data is transmitted directly with minimum no. of nodes in the entire transmission path. But if user chooses for least cost transmission then it would be transmitted through the path which may contain more number of nodes but path cost is least.

The main idea is to use the network graph and the associated link weights to produce a small set of backup network configurations. The link weights in these backup configurations are manipulated so that for each link and node failure, and regardless of whether it is a link or node failure, the node that detects the failure can safely forward the incoming packets towards the destination on an alternate link. It assumes that the network uses shortest path routing and destination based hop-by-hop forwarding.

This configuration is designed into three steps which can be described as:

1. Create a group of backup configurations that could be utilized by every net setup component expelled from data packet forwarding in every setting.
2. For every setting an average routing algorithm just as Open shortest path first (OSPF) is employed, which helps to analyze configuration of shortest paths and for creating forward tables to each of the router, which is also based on the configuration of the routers. The main advantage of that routing algorithm is that it will guarantee a loop- free and successful flow in forwarding the data within one configuration of the router.
3. Design a forwarding procedure that will make available an advantage of the backup configurations which will be ready to lend a hand to provide fast recovery from a constituent breakdown.

In this approach, for all connections and systems in the network the backup configuration is designed, which is configured in the way that connection or network system is not employed to forward traffic and for every transfer on its own connection or node breakdown, there will be a offered setting that will route the network traffic from the start point to its objective on an alternate path and will also help to avoid the failed element, and for that reason there is to design a suitable path with a finite rate flanked by every network node combination .

The concept permits data packet onward to keep on over already configured substitute later hops directly just subsequent to the discovery of the breakdown. It provides a full security of revival from any sole connection or node breakdown, which comprises a huge middle-of-the-road of the breakdowns veteran in any network.

Conclusion

Our proposed concept is essential for any networks which are based on single path architecture. In this paper we propose to introduce a concept

which would be efficient enough to handle path or node failure scenarios and would make transmissions flawlessly. For an evaluation simulation can be carried out to check for the consistency of data on destination machine as it should be 100% same as it was sent from the source machine.

References

[1] *Adamou M and Sarkar S, (2002), "A Framework for Optimal Battery Management for Wireless Nodes", Proceedings of IEEE INFOCOMP 2002, pp. 1783-1792.*

[2] *Al-Kofahi O.M and Kamal A.E, (2007), "Network Coding-Based Protection of Manyto-One Flow Networks", Mobile Adhoc and Sensor Systems, IEEE international Conference.*

[3] *Biswas S and Morris R, (2005), "ExOR: Opportunistic Multihop Routing for Wireless Networks", Proceedings of the 2005 conf. ACM SIGCOMM, 133-144.*

[4] *Chen, Shigang and Nahrstedt K (1999), "Distributed quality-of-service routing in adhoc networks", Selected Areas in Communications, IEEE Journal on.17, 1488-1505.*

[5] *Dong Q, Banerjee S, Adler M, and Misra A, (2005), "Minimum Energy Reliable 19 Paths Using Unreliable Wireless Links", International Symposium on Mobile Ad Hoc Networking & Computing, Proceeding of the 6th ACM International symposium on Mobile ad-hoc networking and computing, 449-459.*

[6] *Dilmaghani R.B and Rao R.R, (2007), "Future Wireless Communication Infrastructure with Application to Emergency Scenarios", World of Wireless, Mobile and Multimedia Networks, 2007. WoWMoM 2007. IEEE International Symposium.*

[7] *Draves R, Padhye J and Zill B, (2004), "Comparison of Routing Metrics for Static Multihop Wireless Networks", Proceedings of the 2004 conference on Application, Technologies, architectures, and protocols for computer Communications, SESSION: Wireless and delay-tolerant networks. 133-144.*

[8] *Draves R, Padhye J And Zill B, (2004), "Routing in Multi-Radio, Multi-Hop wireless Mesh Networks", Proceedings of the 10th annual international conference on Mobile computing and networking, SESSION: Algorithms for multihop networks. 114-128.*

[9] *Ganesan D, Govindan R, Shenker S and Estrin D, (2001), "Highly-resilient, energy-efficient multiple routing in wireless sensor networks", ACM SIGMOBILE Mobile Computing and Communications Review. 5(4), 11-25.*

[10] *Garcia-Luna-Aceves J. J And Madruga E.L, (1999) "Core assisted mesh protocol", Selected Areas in Communications, IEEE Journal on. 17(8), 1380-1394.*

[11] *Gerla M, Hong X, And Pei G, (2002), "Fisheye state routing protocol for ad-hoc networks", IETF Internet Draft, draft-irtf-manet-fsr-03.txt.*

[12] *Narvaez P, Siu K.-Y and Tzeng H.-Y, (1999), "Local restoration algorithms for Link-state routing protocols", in Proc. IEEE Int. Conf. Computer Communications and Networks (ICCCN'99), pp. 352–357.*

[13] *Nelakuditi S, Lee S, Yu Y, Zhang Z. L and Chuah C. N, (2007) "Fast local Rerouting for handling transient link failures", IEEE/ACM Trans. Networking, vol.15, no. 2, pp.359–372.*

[14] *Noguchi T, Matsuda T, and Yamamoto M, (2003), "Performance evaluation of new multicast architecture with network coding", IEICE Trans. Commun, vol. E86-B, pp. 1788–1795.*

[15] *Nucci A, Schroeder B, Bhattacharyya S, Taft N, and Diot C, (2003.),"IGP link weight assignment for transient link failures," in Proc. 18th Int. Teletraffic Congress,Berlin, Germany.*

[16] *Sridharan A and Guerin R, and Diot C, (2005), "Achieving near-optimal traffic Engineering solutions for current OSPF/IS-IS networks", IEEE/ACM Trans.Networking, vol. 13, no. 2, pp. 234–247.*

[17] *Toh C. K, (2001), "Maximum Battery Life Routing to Support Ubiquitous Mobile Computing in Wireless Ad hoc Networks", IEEE Communications Magazine, vol.39, no. 6, pp.138-147.*