Indonesian Journal of Electrical Engineering and Informatics (IJEEI)
Vol. 4, No. 3, September 2016, pp. 176~180
ISSN: 2089-3272, DOI: 10.11591/ijeei.v4i3.223

A Study on IP Network Recovery through Routing Protocols

K Karthik*[1], T Gunasekhar[2], D Meenu[3], M Anusha[4]
[1,2,4]Dept of Computer Science and Engineering, K L University, Vijayawada, Vaddeswaram 522502, India
[3]Dept of Computer Science and Engineering, Ideal College of Engineering, Kolkata, India
*Corresponding author, e-mail: kkarthik46@gmail.com[1], meenudonka@gmail.com[3]

Abstract

Internet has taken major role in our communication infrastructure. Such that requirement of internet availability and reliability has increasing accordingly. The major network failure reasons are failure of node and failure of link among the nodes. This can reduce the performance of major applications in an IP networks. The network recovery should be fast enough so that service interruption of link or node failure. The new path taken by the diverted traffic can be computed either at the time of failures or before failures. These mechanisms are known as Reactive and Proactive protocols respectively. In this paper, we surveyed reactive and proactive protocols mechanisms for IP network recovery.

Keywords*: Proactive protocol, Reactive protocol, IP network recovery*

1. Introduction

Network which contains many network components of both hardware and software can incur failures due to one (or even multiple) of its contained components incurs a failure, as shown in Figure 1. Ranging from the largest to the smallest and from hardware to software, network failures can be divided into the following categories [1] [2]:

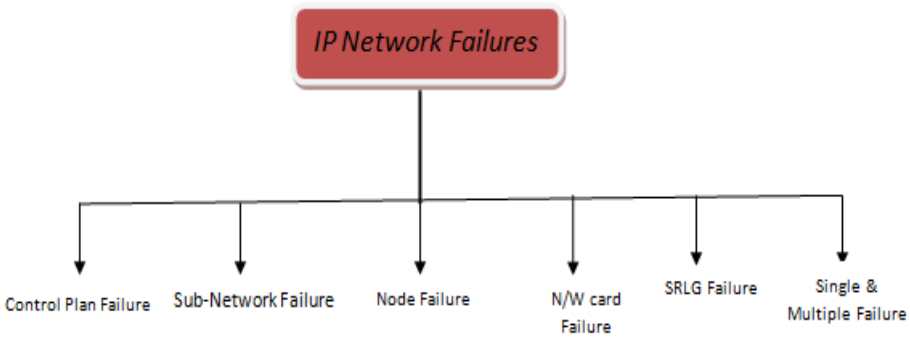

Figure 1. IP Network Failure Classification

Control plane failure

This type of failure is mainly related to software, i.e., network control plane software. For example, in a GMPLS-based network which is made up of a control plane and data plane, the control plane failure would lose the control of the data plane, which means that we cannot establish new service connections, or terminate or modify an existing service connections within the data plane, even though the existing connections can still perform normally to carry user's data [3].

Sub network failure

This is a type failure occurred with a regional sub network that commonly shares a risk, e.g., a region that has high occurring frequency of earthquake. In addition, some large disasters such as flooding, tsunami, etc. can also disable a regional sub network [4].

Received October 17, 2015; Revised June 15, 2016; Accepted July 2, 2016

Node failure

This is a type of failure occurred with a single network node. The reasons for this kind of failure include accidents or disasters at a network operational center, such as power shutdown due to fire, flooding, etc [5].

Network card failure

Network card failure is a type of failure under the umbrella of the node failure type.

Link failure

link failure in general is the most common network failure that occurs due to fiber cut.

SRLG failure

SRLG failure is a generic concept to define all types of network failures whenever a common SRLG incurs a failure. Here a SRLG can be a fiber link, node, sub network, or control plane, etc.

Single failure and multiple failures

In general network failure implies a single network failure because network failure normally seldom occurs. However, under some situations, there can be more than failure occurring with a network. This kind of situation is called multiple failures [6] [7].

2. Proactive Protocols

Number of techniques has been proposed for local and fast protection in IP networks. It doesn't require any notification to neighbor node after failure. A router on detection of failure will redirect traffic to backup paths right away instead of waiting for the completion of network-wide routing convergence [8] [9].

O2 Routing

A network is configured in such a manner that all nodes have two valid next-hops to all destinations. Traffic is split between the next-hops in the normal case, and they function as backup for each other in case of a failure. To avoid loops, some links are excluded from packet forwarding for certain destinations in the normal case, and are only used as backup. O2 requires well connected network topology to give complete protection [10].

Failure Insensitive Routing (FIR)

In FIR mechanism, routers are not explicitly made aware of a failure through notification messages. Instead, they infer that a link failure if a packet for a given destination arrives at an unusual interface.

Loop Free Alternatives

The basic idea behind Loop Free Alternates is to use a precompiled alternate next hop that will not loop the packets back to the detecting node or to the failure in the event of a link failure so that traffic can be routed through this alternate next hop when a failure is detected [20].

NotVia Addresses

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. It is complex because it uses tunneling [19].

Multiple Routing Configurations (MRC)

Multiple Routing Configurations (MRC) is a proactive and local protection mechanism. MRC is based on enervating back up configurations. Back up configurations are generated in such a way that for all links and nodes in the network, there is a configuration where that link or node is not used to forward traffic. Thus, for any single link or node failure, there will exist a

configuration that will route the traffic to its destination on a path that avoids the failed element [10] [11].

3. Reactive Protocols

In this type of routing protocol, each node in a network discovers or maintains a route based on-demand. It floods a control message by global broadcast during discovering a route and when route is discovered then bandwidth is used for data transmission [18]. The main advantage is that this protocol needs less touting information but the disadvantages are that it produces huge control packets due to route discovery during topology changes which occurs frequently in MANETs and it incurs higher latency. The examples of this type of protocol are Dynamic Source Routing (DSR) [12] [13].

3.1. Ad-hoc On demand Distance Vector (AODV)

AODV is distance vector type routing where it does not involve nodes to maintain routes to destination that are not on active path. As long as end points are valid AODV does not play its part. Different route messages like Route Request, Route Replies and Route Errors are used to discover and maintain links. UDP/IP is used to receive and get messages.. AODV uses a destination sequence number for each route created by destination node for any request to the nodes. Then Route Reply is sent back to the source node. Finally the animator in any simulation has to be discussed. NAM is used in NS2 [13] [20].

3.2. Dynamic Source Routing (DSR)

This is an On-demand source routing protocol. In DSR the route paths are discovered after source sends a packet to a destination node in the ad-hoc network. The source node initially does not have a path to the destination when the first packet is sent. The DSR has two functions first is route discovery (Figure 2) and the second is route maintenance [14]

Different DSR Algorithms

a) Route discovery.
b) Route maintenance.

Assumptions:

a) X, Y, Z, V and W form ad-hoc network.
b) X is the source node.
c) Z is the destination node.

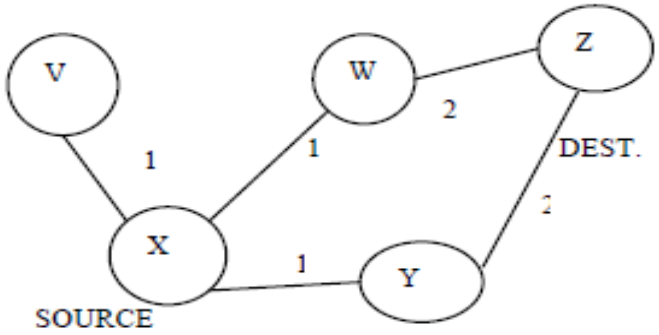

Figure 2. Route discovery

Route discovery algorithm*:*

a) X broadcasts a Route Request Packet with the address of destination node Z.
b) The intermediate nodes V, W, Y receive the Route Request Packet from X, as shown in Figure 2.

c) The receiving nodes V, W, Y each append their own address to the Route Request Packet and broadcast the packet (as shown in Figure 3).
d) The destination node Z receives the Route Request packet. The Route Request packet now contains information of all the addresses of the nodes from source node X to destination node Y.
e) On receiving the Route Request Packet the destination node Z sends a reply called the Route Reply Packet to the source node X by traversing a path of addresses it has got from the Route Request packet.
f) DSR caches the route information for future use.

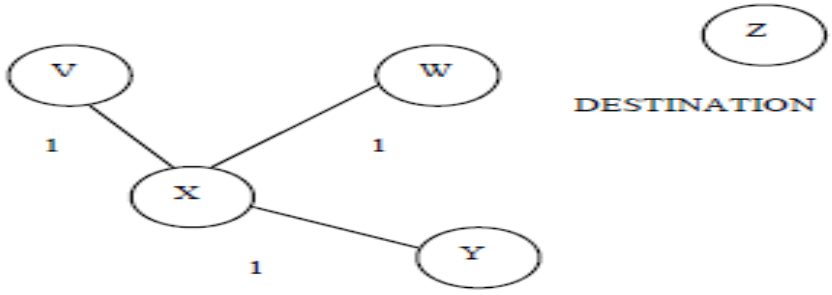

Figure 3. Showing re-broadcasting by nodes V, W, Y

Route Maintenance algorithm [5, 8]

a) In DSR algorithm a link break is detected by a node along the path from node X to node Z, in this case node W.
b) Then node W sends a message to source node X indicating a link break.
c) In this case, node X can use another path like X-Y- Z or it must initiate another route discovery packet to the same destination node, in this case 'Z' [13] [14].

4. Conclusion

The resumption of forwarding after a link failure typically takes seconds. During this period, some destinations could not be reached and the packets to those destinations would be dropped. Proactive mechanism, in which routers compute and store backup paths for potential failures before hand, and once a local link failure is detected, a router will redirect traffic to backup paths right away instead of waiting for the completion of network-wide routing convergence. Proactive routing has short failure recovery time and reduces the overhead of both update propagation and path re-calculation.

References

[1] A Raja, OC Ibe. "A survey of IP and multiprotocol labelswitching fast reroute schemes". *Comput*. 2007; 51(8): 1882-1907.
[2] Amund Kvalbein, Audun Fosselie Hansen, Tarik Ci˘cic, Stein Gjessing, Olav Lysne. "Multiple Routing Configuration for Fast IPNetwork Recovery". *IEEE/ACM Transactions on networking*. 2009; 17(2).
[3] A Markopoulou, G Iannaccone, S Bhattacharyya, C Chuah, C Diot. "Characterization of failures in an IP backbone". in Proc. *IEEE INFOCOM*. 2004: 2307–2317.
[4] C Labovitz, A Ahuja, A Bose, F Jahanian. "Delayed Internetrouting convergence". *IEEE/ACM Trans. Networking*. 2001; 9(3): 293–306.
[5] DD Clark. "The design philosophy of the DARPA internet protocols". *ACM SIGCOMM Comput. Commun. Rev*. 1988; 18(4): 106–114.
[6] A Basu, JG Riecke. "*Stability issues in OSPF routing*". in Proc. ACM SIGCOMM, San Diego, CA. 2001: 225–236.
[7] C Labovitz, A Ahuja, A Bose, F Jahanian. "Delayed internet routing convergence". *IEEE/ACM Trans. Networking*. 2001; 9(3): 293–306.
[8] C Boutremans, G Iannaccone, C Diot. "Impact of link failures on VoIP performance". in Proc. *Int. Workshop on Network and Operating System Support for Digital Audio and Video*. 2002: 63–71.

[9] D Watson, F Jahanian, C Labovitz. "*Experiences with monitoring OSPF on a regional service provider network*". in Proc. 23rd Int. Conf. Distributed Computing Systems (ICDCS'03), Washington, DC, IEEE Computer Society. 2003: 204–213.
[10] P Francois, C Filsfils, J Evans, O Bonaventure. "Achieving sub-second IGP convergence in large IP networks". *ACM SIGCOMM Comput. Commun. Rev*. 2005; 35(2): 35–44.
[11] A Markopoulou, G Iannaccone, S Bhattacharyya, CN Chuah, C Diot. "Characterization of failures in an IP backbone network". in Proc. *IEEE INFOCOM*. 2004; 4: 2307–2317.
[12] S Nelakuditi, S Lee, Y Yu, ZL Zhang, CN Chuah. "Fast local rerouting for handling transient link failures". *IEEE/ACM Trans. Networking*. 2007; 15(2): 359–372.
[13] S Iyer, S Bhattacharyya, N Taft, C Diot. "An approach to alleviate link overload as observed on an IP backbone". in Proc. *IEEE INFOCOM*. 2003: 406–416.
[14] S Rai, B Mukherjee, O Deshpande. "IP resilience within an autonomous system: Current approaches, challenges, and future directions". *IEEE Commun. Mag*. 2005; 43(10): 142–149.
[15] Gunasekhar T et.al. "A Survey on Denial of Service Attacks". *International Journal of Computer Science and Information Technologies*. 2014; 5(2): 2373-2376.
[16] Anusha M, Srikanth Vemuru, T Gunasekhar. "Transmission protocols in Cognitive Radio Mesh Networks". *International Journal of Electrical and Computer Engineering (IJECE)*. 2015; 5(4).
[17] Gunasekhar T, Rao KT, Basu MT. "Understanding insider attack problem and scope in cloud". *2015 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*. 2015; 1(6).
[18] Anusha M, Vemuru S, Gunasekhar T. "TDMA-based MAC protocols for scheduling channel allocation in multi-channel wireless mesh networks using cognitive radio". *2015 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*. 2015: 1, 5.
[19] Gunasekhar T et.al. "Mitigation of Insider Attacks through Multi-Cloud". *International Journal of Electrical and Computer Engineering (IJECE)*. 2015; 5.1): 136-141.
[20] M Dileep Kumar, M Trinath Basu, T Gunasekhar. "Meshing VANEMO protocol into VANETs". *International Journal of Applied Engineering Research*. 2015; 10(12): 31951-31958.
[21] R Praveen Kumar, Jagdish Babu, T Gunasekhar, S Bharath Bhushan. "Mitigating Application DDoS Attacks using Random Port Hopping Technique". *International Journal of Emerging Research in Management &Technology*. 2015; 4(1): 1-4.
[22] Gunasekhar T, K Thirupathi Rao. "EBCM: Single Encryption, Multiple Decryptions". *International Journal of Applied Engineering Research*. 2014; 9(19): 5885-5893.
[23] Kalavakolanu Narasimha Sastry, T Gunasekhar. "Novel Approach for Control Data Theft Attack in Cloud Computing". *International Journal of Electrical and Computer Engineering (IJECE)*. 2015; 5(6): 2088-8708.