ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Indian Journal of Science and Technology, *Vol 9(2), DOI: 10.17485/ijst/2016/v9i2/76183, January 2016*

A Mathematical Approach to Improve the Network Performance

Rohit N. Devikar[1]*, D. V. Patil[2] and V. Chandraprakash[1]

[1]Department of Computer Science and Engineering, K. L. University, Vaddeswaram, Guntur - 522502, Andhra Pradesh, India; rohit.devikar89@gmail.com, vchandrap@kluniversity.in

[2]Department of Computer Engineering, R. H. Sapat College of Engineering, Nasik - 422005, Maharashtra, India; dipakvpatil17@gmail.com

Abstract

Objectives: Nowadays the Internet has become vital to each and every one. It is sensitive to link failures and node failures due to many reasons in the network connectivity. Any change in the node or link may change the routing table of many nodes. Due to this change, the routing table of many nodes may be unstable. These failures lead to increase the convergence time of network. The paper focused on reducing the convergence time of network. **Methods**-In this research paper, we have proposed a novel approach that keeps the value of Minimum Route Advertisement Interval (MRAI) timer fickle. In this approach, depending on the position of receiver, the value of the MRAI timer is varying. In this research, if more than one route is available to reach the destination then we have used the soft computing approach so that the load is balanced over all the paths that are reaching to the destination to avoid the congestion. **Result:** The approach used in this paper focuses on fast network convergence and maximum link utilization. The Fickle MRAI used in the network for reducing the convergence time up to 5 second, also the use of load balancing approach to improve link utilization of the network. **Conclusion:** The proposed work improves fast network convergence and utilization of bandwidth as the traffic flows from the entire shortest paths in the network.

Keywords: Autonomous System, Border Gateway Protocol, Congestion Control, Load Balancing

1. Introduction

Route vector protocol i.e., Border Gateway Protocol consists of nodes which are used to select and exchange the path where to send the traffic. We have the query of following questions: What is the impact of route failure or any link failure on the availability of the network, for finding the paths? The answer is not clear because some paths that are allowed by routing policies may get hidden by route vector protocol. In[1] developed an algebraic theory to address the above questions. In particular, author in characterize a wide class of routing policies for which they can calculate in polynomial time a least number of links whose failure leaves a path vector protocol without a communication route from one node to another[1]. The theory is applied to all the available description of the Internet topology to measure how much of its intrinsic connectivity is lost because of traditional peer-peer routing policies, customer-provider and how much can be regained with simple alternative policies.

For the inter-domain communication we require the Autonomous Systems (ASs). What is meant by Autonomous System? Why there is a necessity for evolution of this Autonomous System. The answer for this question depends upon the scalability of the internet. In old era, the internet users were very small in numbers and also the cost required for the internet uses were also very high. Due to small number of users, handling them was

Author for correspondence

very simple. But in new era, number of internet users has increased rapidly so handing of them is quite difficult. To resolve this issue the generation of Autonomous System has taken place. Each Autonomous System in the network is distinguished by using Autonomous System Number (ASN).

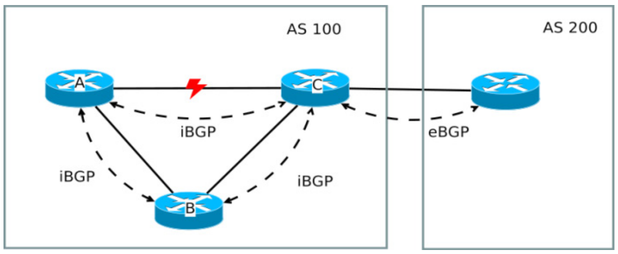

Figure 1. Autonomous Systems.

Figure 1 shows the two Autonomous Systems, AS 100 and AS 200. Each user within the Autonomous System is communicated by using Intra-Domain Routing protocol such as RIP, OSPF, and IGRP. For the communication between the Autonomous Systems we require a special type of protocol called as Border Gateway Protocol (BGP). In the Internet, numbers of Autonomous Systems are present and they are communicated using the BGP Protocol.

Communication between the two ASs is carried out using a gateway routers called as speaker node. Speaker node advertises its AS routing table with the connected speaker nodes of other ASs. After each 30 seconds of period each speaker node advertises its routing table. The convergence time is the time required for the speaker node to update its table with the network. The convergence time should be minimum so that each speaker node is updated with the network changes as soon as possible. Due to this the availability of the network increases and transmission is at faster rate.

The paper reduces the convergence time and increases the availability of the network. Also shows how to balance the load in the network using Algorithm.

In the recent years internet instability and route fluctuation are important problems in the network. Instability in the network results in loss of packets which in turn increases the latency and convergence time. Following section describes the research work done by several researchers to improve the convergence time and instability of the network.

In[2] described some unpredicted trends in routing stability. The authors developed the taxonomy for routing information and for identifying the origin of pathological behavior. The routing information is classified into three classes: 1. Forwarding instability, 2. Policy Fluctuation, 3. Pathologic updates (redundant). This research observed redundant data during update of routing topology for nine months. Most of the data collected were redundant. Finally they explained the impact of this redundant data on network infrastructure. In[3] defined a failure probability technique to improve the stability of the network. Each link has the failure probability *Pi*, and each path is independent of others, no any node or link is common for particular path in the network. In mobile network, the topology changes due to time unstable state of the network. As this scheme defines the probability of path failure for each link, it is used to develop the probability function *Psucc* (Probability that no more Mblocks is lost). From observation it was shown that the probability of successful communication increased between source and destination only when we increase the number of paths. This reduces the congestion and transmission delay. In the recent years OSPF and IS-IS are used to compute the Shortest Path Tree (SPT) from router to router. As there are multiple SPT in the network, recovery from failure causes changes in existing SPT topology which results in routing instability. In[4,5] proposed the new algorithm which improves the stability of network by making minimum changes in the existing SPT topology when some link or router in the network fails. After failure, the discontinuity is encountered in link state advertisement and re-computation of routing table. For link state routing OSPF (Optimal Shortest Path First) protocol is used. As failures are increasing, the instability in the network increases. To improve the failure resiliency without affecting routing stability; in[6] proposed a Failure Insensitive Routing (FIR) approach. This approach suppresses the link state advertisement. Using this approach, when at most one link failure notification is suppressed, a packet is guaranteed to be transmitted to its destination along loop free path. The experimental results show that FIR provides better routing stability and availability than OSPF in terms of network sizes, failure frequency, and convergence delays.

In[7] reported the results on efficiency and stability to achieve the traffic engineering objectives in inter domain routing when interactions among routing to multiple destinations cause instability in routing even if each route to destination has unique solution. Route selection problem is stable only if the interaction among the

ISPs follows the set of inter domain traffic engineering guidelines; otherwise instability occurs in route selection process. The accidental activities such as failure, misconfiguration, route flapping, induced several BGP instabilities in the network lead to delays, loss of data and connectivity.

Today's internet routers are overcome by a number of BGP updates caused by events such as failure, session reset, and policy changes. Such events can delay routing convergence, which degrades the performance of networks in terms of jitter and delay sensitive application. In[8] proposed the novel approach of differentiated processing in terms of BGP updates, which improve the routing convergence and reduces the routers load. Based on this approach the BGP updates are classified into two classes. Higher priority updates are processed sooner, while the lower priority updates are delayed to reduce router load and processing. The simulation result shown reduces the convergence time by 80% and having 30% fewer BGP updates. Mean Route Advertisement Interval (MRAI) performs an important role in BGP convergence time. In the case of normal load, adaptive MRAI timers perform better for BGP updates. As soon as load is increased there may be a problem of flooding at routers and adaptive MRAI timer is not efficient. Adaptive MRAI timer fails to scale if the BGP updates in the network are increasing. In[9] proposed the BGP instability detection mechanism that can be executed by individual routers. The input data for detection of instability is BGP update messages received by routers from its neighbor. From this BGP update messages features (like AS path length, AS path edit distance) are extracted in every five minutes, this shows the change in topology. The GLR (Generalized Likelihood Ratio test), Segmentation boundary detection, Boundary position optimization algorithms are used to detect the changes. In[10] proposed a Path Exploration Damping (PED) technique which reduces the volume of BGP update messages and decreases the average time required to restore reach-ability. They compare PED impact on convergence time with Mean Route Advertisement Interval (MRAI), Route Flap Damping (RFD), and Withdrawal Rate Limiting (WRATE). From experimental results it was found that the total BGP announcement can decrease by up to 32%, and path exploration reduced by 77% compared with traditional MRAI approach. In[11] compared different techniques like Fast Reroute one to one backs up, local rerouting, Haskin, 1+1 path protection recovery mechanism and PSL oriented path protection mechanism technique for fast rerouting after failure. The performance shows that 1+1 path protection recovery mechanism has minimum packet loss, but having more cost. In[12] proposed the FLD-MRAI (Flexible Load Dispersing MRAI) algorithm that disperses the load in the network, which results in reducing the routers overhead. The authors focused on routing policies and their effects on number of updates and convergence time. The FLD-MRAI algorithm works in case of both high and normal loads. When Degree of Preference (DoP) chooses the shortest path, then FLD-MRAI believe this situation as normal load, and when DoP chooses the longest path then FLD-MRAI believe this situation as high load.

In[13] presented a new parallel lookup model called split routing lookup model rather than looking for optimization techniques for traditional lookup model. In this model, all the prefixes are split to produce redundancies and after that they are removed during information integration. The splitting of prefixes reduces routing updates; also this model can be used for parallel processing for lookup address. In[14] have proposed a technique called source directed path diversity using which, sources can give alternate paths to forward the traffic. In packet header, sources specify the tag called as Source Directed Tag (SDT) that informs BGP routers for path selection. BGP routers on the basis of Source indication, forward the traffic independently on the indicated path. In order to address the link failure between Autonomous Systems in[15] has proposed a fast reroute scheme by incorporating Software Defined Networking (SDN) with BGP called Software Defined Autonomous System level Fast Rerouting (SD-FRR). By considering routing policies SD-FRR aims to provide policy compliant path to protect forwarding of data locally, which avoids packet losses and efficiently improves the network availability.

In[16] proposed a Hot Potato routing technique works on the basis of link weights and link failure. The Figure 2 shows router A will choose the egress router C to travel the traffic to different ASs. Suppose distance between A->C changes from 9 to 11 intentionally or link between A->C failed due to some interruption. Although the distance between A->C changes, still there is a path between A->C available but has a large distance. A chooses the path A->B to forward the traffic. This routing which changes the path dynamically is called hot potato routing. The routing in the network is flexible and visible to all neighbors in the network, which is efficient to improve the network convergence. But Hot Potato technique has the chances of packets loss due to

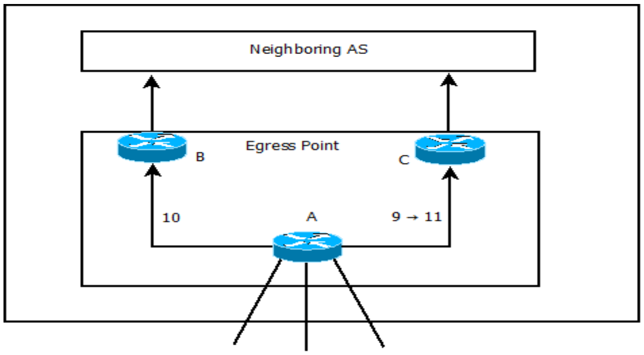

Figure 2. Hot potato routing changes from C to B.

slow convergence of BGP. In[17] introduced a Novel Traffic Dividing and Scheduling (NTDS) mechanism; it is used to disseminate traffic across circuits, based on each circuit congestion level, bandwidth capacity, latency and throughput. In[18] have proposed a green networking technique in addition to hot potato called HOTPLEC that shutdown the least utilized links or routers during off peak hours. Shutdown of unutilized links or routers reduces the energy consumption of network without negative impact on BGP. In[19] proposed a tunneling mechanism which is useful for providing a loop free routing between different organizations. The below section describes the algorithms to improve the performance of the networks.

2. Proposed Work

2.1 Convergence Time

The main factor that affects convergence time is the MRAI value. The default value of MRAI timer is 30s. MRAI value depends upon links delays and length of the path reaching to the destination. But whenever the sum of delays exceeds default value of the MRAI timer, default value will be used for network advertisement. The purpose of this is not to use the default value every time because it will increase network convergence time and also degrade the network performance. Therefore the value of MRAI may fluctuate up to a maximum of 30s.

The following algorithm sets the value of MRAI timer.

$$\sum P_i = (p_1, p_2, p_3 \dots \dots \dots p_n)$$

Where P_i is i^{th} path reaching to destination.

$$P_1 = \sum R_1$$

$$\sum R_1 = (r_1, r_2, r_3 \dots \dots \dots r_n)$$

R_1 = Total number of routers available on path P_i.
$L(P_i)$ = $(l_1, l_2, l_3, \dots\dots l_d)$.
$L(P_1)$ = Total number of links present in path P_1.
$D[L(P_i)]$ = D $(l_1, l_2, l_3, \dots\dots l_d)$.
$D[L(P_1)]$ = Total delay in the links on path P_1.
$W(P_i)$ = W $((l_1, l_2, l_3, \dots\dots l_d))$.
$W(P_1)$ = Total processing time on path P_1.
$Q[R(P_i)]$ = Q $(q^r{}_1, q^r{}_2, q^r{}_3, \dots\dots q^r{}_d)$.
$Q[R(P_1)]$ = Total queuing delay at each router on path P_1.
Maximum delay (TD) = $D[L(P_i)]+W(P_i)+Q[R(P_i)]$.
MRAI = TD.
If (TD> = Default MRAI)
{
MRAI = Default MRAI;
}
Else
{
MRAI = TD;
}

After the convergence of network it is necessary to apply load balancing approach to improve the utilization of each and every link reached to destination.

2.2 Load Balancing Approach

The proposed work improves load balancing and network availability. In the network, for switching the traffic a primary path (p1->pi) as well as a number of alternative paths is available. In traditional approach only primary path is utilized and available alternate paths remains idle. Due to the high utilization of primary path, congestion occurs in the route. To avoid this congestion, it is necessary to traverse traffic through alternate paths also. The proposed work shows that how we can improve the network availability by balancing the load on the primary as well as on alternate paths. If there are only two paths available for destination then use Algorithm1, otherwise use Algorithm 2.

Algorithm 1
Step 1: Initialize
P:Total routes=2
P1 = Path 1

P2 = Path 2

S = Source Router

D = Destination Router

R = Total number of routers between source and destinations

R1= Routers in path r1.

R2= Routers in path r2.

N = Total number of packets.

Step 2: **R**= (∑ Path 1 Routers between source and destination) + (∑ Path 2 Routers between source and destination)

Step 3: **Z**=No. of Packets at the Source router (N)/R;

Step 4: Else

{

If (P1 Hops >P2 Hops)

Then P1 sends (Z*∑R2) number of packets.

}

Step 5: Else

{

If (P2 hops >P1 hops)

Then P2 sends (Z*∑R1) number of packets.

}

Step 6: Else

Both P1 and P2 send N/2 number of packets.

The result analysis shows how the algorithm balanced the network traffic, also shows the efficient utilization of bandwidth.

Algorithm 2

Step 1: **Initialize**

X: Total routes>2

N: Number of packets at source.

n: Total number of paths.

i: Current path

P_i: No. of packets transmitted from i^{th} path

Step2: Calculate Path P_i reaching to the destination.

Step3: i=0;

Step4: do

{

i++;

$$\underset{(i \in n)}{P_i} = \sum_{i=1}^{n} \left[\frac{N}{2i} - \frac{i(i-1)}{2} \right]$$

S = *N-Pi;*

Print (“The Packet Transmitted from Path P_i”= S);

} while(R(P_i)+5<R($P_{(i+1)}$)&&(i< = n))

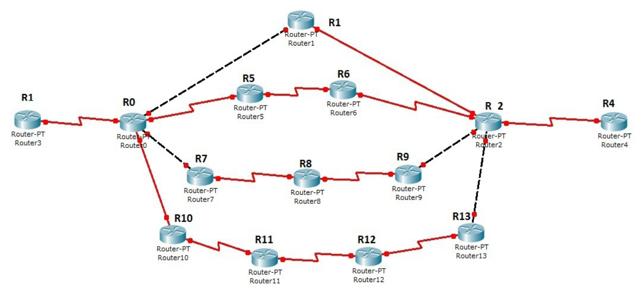

Figure 3. More than two routes available from source (S) to destination (D).

Step5: If(s>0)

{

Send S packets from Path P1;

}

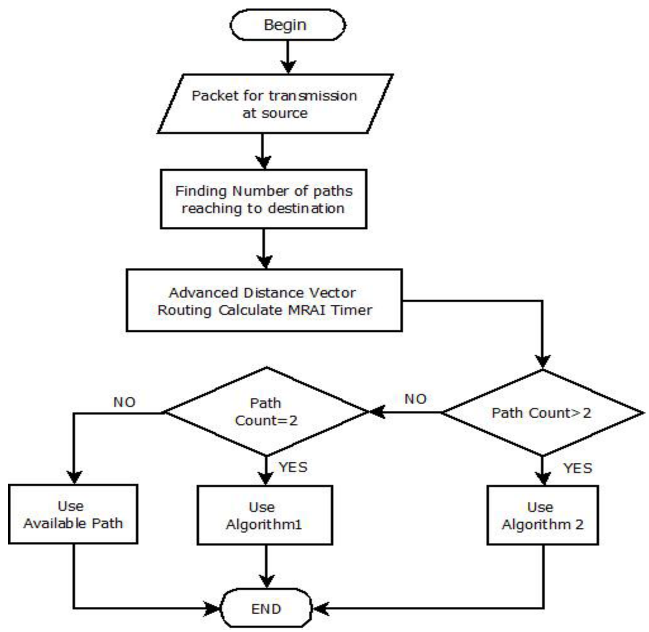

Figure 4. Flowchart to improve convergence time and link utilization.

The Algorithm 1 and Algorithm 2 show the full utilization of bandwidth. If only two routes are available then use Algorithm 1, and if more than two routes are available for destination then we use the Algorithm 2. The Figure 4 shows a flowchart that discusses the overall idea of improving convergence time and link utilization.

3. Result Analysis

Figure 5 shows that there are two paths for destination: PATH 1 and PATH 2.

Source S requires 5 hops to reach to the destination D through PATH 1 and requires 3 hops to reach to the destination D through PATH 2. Suppose source have "x" packets for destination D.

By using Algorithm 1:

Total number of routers between source S and destination D in PATH 1 and PATH 2 are TR i.e., R = TR; R1 = a, R2 = b, N = x.

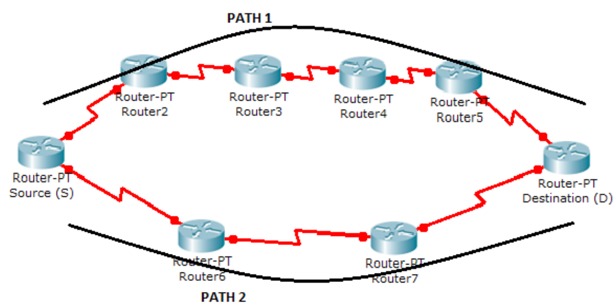

Figure 5. Two routes available from source (S) to destination (D).

Z = N/R = x/TR.

So Source S sends ((x/6)*∑R2) number of packets from PATH 1, and sends ((x/6)*∑R1) number of packets from PATH 2.

3.1 Packet Transfer V/S Number of Path

From Figure 5 it has been noticed that if source S has 90 packets for transmission then it will send 60 packets from primary path and 30 packets from alternate path respectively. Figure 6 shows packets transmitted from primary as well as alternate path.

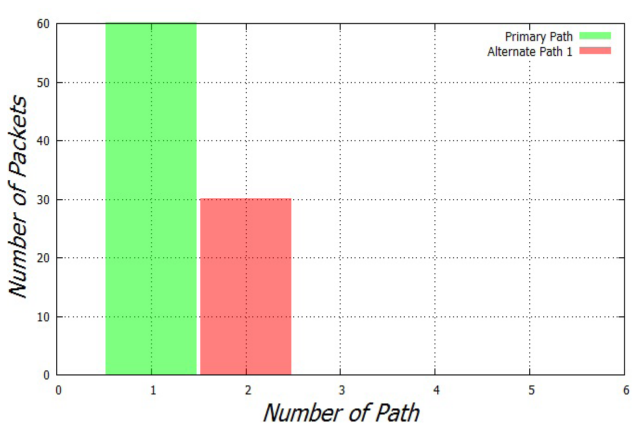

Figure 6. Number of packets transmited via Path 1 and Path 2 from Source S for Algorithm 1.

If topology consists of more than two paths for destination as shown in Figure 3, then transmit the packets from primary as well as from all the alternate paths to improve link utilisation. Table 1 and Figure 7 reflects the number of packets transmitted from primary as well as from all the alternate paths.

From Figure 5 traditional approach shows that when the source has data or packets for destination then it follows the shortest path i.e., Path 2. As it has only two routers between source and destination, there is a possibility for increasing the traffic on path 2 after some time interval so path 2 gets congested, and the source decides to move the traffic from alternate path i.e., Path 1. After some time interval there is again a possibility for the congestion in Path 1. So forwarding the traffic from path 2 takes place and this is called as Route Flapping or Route Oscillation and there is a need to reduce this flapping. Also when the traffic flows from Path 2, the Path 1 is idle and vice versa, which reduces the utilisation of bandwidth, results in reduced network performance. These can be overcome by balancing the load over all the links those reach to the destination. Figure 7 shows distribution of packets from all the paths of scenario.

Table 1. Number of packets transmitted from all the paths

Sr.No.	Path	Route	Packet Transmitted
1	P1	R3-R0-R1-R2-R4	51
2	P2	R3-R0-R5-R6-R2-R4	22
3	P3	R3-R0-R7-R8-R9-R2-R4	12
4	P4	R3-R0-R10-R11-R12-R13-R2-R4	05

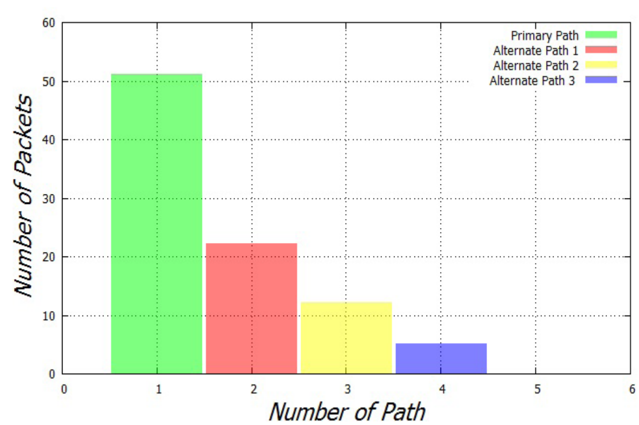

Figure 7. Number of packets transmited from primary as well as from alternate paths.

3.2 Execution Time Vs Link Utilisation

The graph shows utilisation of link over multiple paths. For a given scenario in Figure 3, if we apply the distance vector routing, it has been noticed that path 1 has 100% link utilisation, but remaining alternate paths remain unutilised (0% utilisation) until PATH 1 fails shown in Figure 8 and Algorithm 2 shows proper utilisation of links from primary as well as from alternate paths presented in Figure 9.

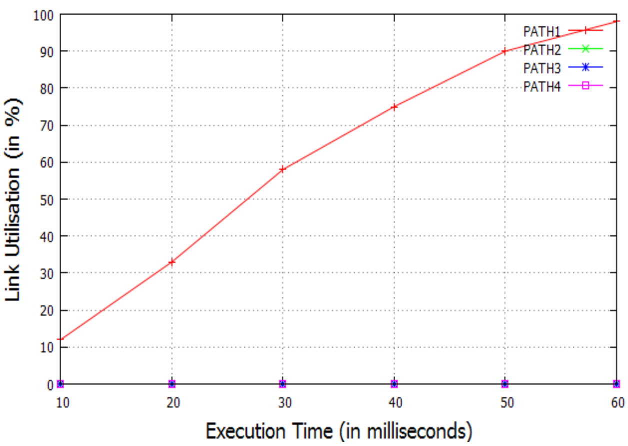

Figure 8. Link utilization in distance vector routing protocol.

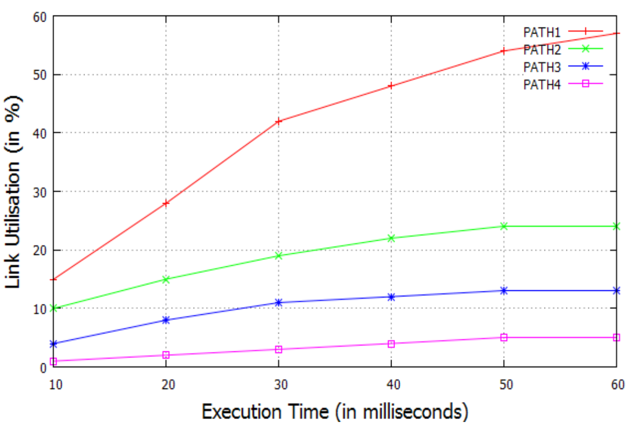

Figure 9. Link utilization in Advanced Distance vector routing protocol.

3.3 MRAI Vs Convergence Time

Figure 10 shows convergence time varies with respect to MRAI interval for default as well as fickle MRAI approach.

The convergence time is directly proportional with the MRAI timer. The convergence time increases with increasing MRAI value. Also, the number of updates decreases with increasing MRAI value. The graph shows two diferent approaches for increasing MRAI values with respect to number of updates. The below graph shows the fickle MRAI has more number of updates than default MRAI value. So, to improve the network availability and for fast network convergence it is necessary to keep the value of MRAI timer less.

3.4 MRAI Vs Convergence Time

Figure 10 shows convergence time varies with respect to MRAI interval for default as well as fickle MRAI approach. The convergence time is directly proportional with the MRAI timer. The convergence time increases with increasing MRAI value. Also, the number of updates decreases with increasing MRAI value. The graph shows two diferent approaches for increasing MRAI values with respect to number of updates. The below graph shows the fickle MRAI has more number of updates than default MRAI value. So, to improve the network availability and for fast network convergence it is necessary to keep the value of MRAI timer less.

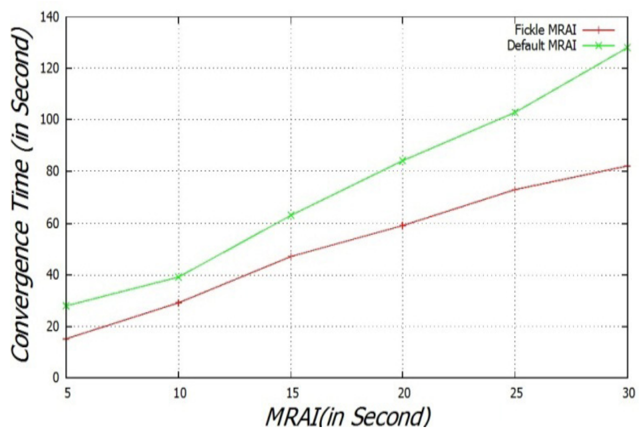

Figure 10. Effect of MRAI timer on convergence time.

4. Conclusion

The congestion in the network is reduced by balancing the load over the paths that reach to the destination. Also the route flapping in the network can be avoided using the proposed algorithm. The proposed work improves the utilization of bandwidth as the traffic flows from the entire shortest paths in the network.

Future work will show that balanced load in multi-homed BGP network will reduce the routing table entry and will improve the route selection process. Also the use of BGP locator/identifier selection protocol will decrease the number of routes seen on the global BGP table and this will improve the popularity of the load balancing.

5. References

1. Sobrinho JL, Quelhas T. A theory for connectivity discovered by routing protocols. IEEE/ACM Transaction on Networking. 2012; 20(3):677–89.
2. Labovitz C, Malan GR, Jahanian F. Internet routing instability. IEEE/ACM Transactions on Networking. 1998; 6(5):515–28.
3. Tsirigos A, Zygmunt JH. Multipath routing in the presence of frequent topological changes. IEEE Communications Magazine. 2001; 39(1):132–8.
4. Narvez P, Siu KY, Tzeng HY. New dynamic algorithms for shortest path tree computation. IEEE/ACM Transactions on Networking. 2000; 8(6):734–46.
5. Narvez P, Siu KY, Tzeng HY. New dynamic SPT algorithm based on a ball-and-string model. IEEE/ACM Transactions on Networking. 2001; 9(6):706–18.
6. Nelakuditi S, Lee S, Yu Y, Zhang ZL, Chuah CN. Fast local rerouting for handling transient link failures. IEEE/ACM Transactions on Networking. 2007; 15(2):359–72.
7. Yang YR, Xie H, Wang H, Silberschatz A, Krishnamurthy A, Liu Y, Erran Li. On route selection for interdomain traffic engineering. IEEE Network. 2005; 19(6):20–7.
8. Sun W, Mao ZM, Shin KG. Differentiated BGP update processing for improved routing convergence. 14th IEEE Conference on Network Protocol ICNP'06; Santa Barbara, CA. 2006 Nov 12-15. p. 280–9.
9. Deshpande S, Thottan M, Ho TK, Sikdar B. An online mechanism for BGP instability detection and analysis. IEEE Transactions on Computers. 2009; 58(11):1470–84.
10. Huston G, Rossi M, Armitage G. A technique for reducing BGP update announcements through path exploration damping. IEEE Journal on Selected Areas in Communications. 2010; 28(8):1271–86.
11. Hariyawan MY. Comparison analysis of recovery mechanism at MPLS network. IJECE. 2011; 1(2): 151–60.
12. Gill R, Paul R, Trajkovic L. Effect of MRAI timers and routing policies on BGP convergence times. 2012 IEEE 31st International Conference Performance Computing and Communications, IPCCC; Austin, TX. 2012 Dec 1-3. p. 314–23.
13. Li Y, Zhang D, Huang K, He D, Long W. A memory-efficient parallel routing lookup model with fast updates. Computer Communications. 2014; 38(1):60–71.
14. Miao X, Fu G, Ma R, Huo L. Source-directed path diversity in the interdomain routing. Journal of Networks. 2014; 9(12):3251–62.
15. Li CX, Li X, Li K, Zhang H, Shi YL, Chen SZ. Toward software defined AS-level fast rerouting. The Journal of China Universities of Posts and Telecommunications. 2014; 21(6):100–8.
16. Teixeira R, Shaikh A, Griffin T, Rexford J. Damping BGP route flaps. Journal IEEE/ACM Transactions on Networking. 2008; 16(6):1295–307.
17. Sangeetha1 K, Ravikumar K. A novel traffic dividing and scheduling mechanism for enhancing security and performance in the tor network. Indian Journal of Science and Technology. 2015; 8(7):689–94.
18. Ruiz-Rivera A, Chin K-W, Soh S. A novel framework to mitigate the negative impacts of green techniques on BGP. Journal of Network and Computer Applications. 2015; 48(C):22–34.
19. Achar RK, Babu MS, Arun M. Border gateway protocol performance and its protection against disturbed denial of service attack. Bonfring International Journal of Research in Communication Engineering. 2015; 8(S2):127–32.