CHAPTER 3

STABILIZING THE INTERDOMAIN ROUTING PROTOCOL AFTER FAILURE

In this chapter an approach to stabilize BGP protocol based on the quality of the path has been proposed using the unconventional approach for alternate path selection after a failure of main path. Attributes of scalable link state routing have been used for calculating the link availability and bandwidth availability. The proposed approach performs better in terms of higher available bandwidth, minimum delay, and also with minimum packet drop. Therefore it provides stability in the routing during failures [Kumar and Kumar (2013a)].

3.1. INTRODUCTION

Routing has become an important topic due to the enormous growth in popularity of the Internet. Especially in the field of communication, routing plays an essential role. To exchange information for path selection, routing protocols are required. The internet is hierarchically divided into domains called Autonomous Systems (ASes), each of which is administratively controlled by one organization. To provide routing between these domains, the Internet uses an interdomain routing protocol known as the Border Gateway Protocol (BGP). The distinct networks of the internet utilize the service provided by interdomain routing [Huston et al. (2010)]. The collection of numerous network domains or autonomous systems is known as the internet. Each Autonomous System (AS) consists of a unique AS Number (ASN). Single or multiple IP address prefixes are present in each AS. Network prefix reachability information is exchanged by BGP using ASes [Sanchez and Duan (2010)]. To distribute reachability information, updates are exchanged among the autonomous
systems speaker router. There are three major behavioral assumptions (BAs) involved during the operation of BGP:

i) The information content of an update must be correct and follow protocol rules.

ii) The route to a prefix must be stable.

iii) The route should adhere to the valley-free routing policy [Chang et al. (2011)].

A router running the BGP protocol is known as a BGP speaker. BGP speakers are used as peers or neighbors. They use the connection-oriented protocol provided by TCP for communication. Additional error correction is not required at the transport layer because the TCP is employed in BGP. For the purpose of communication, each pair of BGP neighbors maintains a session. At the IP layer, the BGP peers are directly connected without using any intermediate node. Intermediate routers that do not run BGP help in passing protocol messages to the peers, forming multi-hop sessions. This type of configuration is not seen frequently [Butler et al. (2005)].

The role of the BGP protocol is to provide routing among networks administered by different organizations, which are identified by their autonomous system numbers (ASN). The BGP establishes two types of peering relationships with the routers, external peering and internal peering. External peering is conducted between routers outside autonomous systems, and internal peering is conducted with routers inside autonomous systems. The BGP speaker redistributes reachability information to internal routers running interior gateway protocols, performs best-path computation to install and forward the most appropriate path information, exchanges network reachability information among peers, and applies routing policy to put restrictions on routing behavior.

The BGP is an augmenting and path vector protocol. An announcement message is sent to a BGP speaker when a new route arrives. If the route no longer exists, a withdrawal message is
sent. Prior to advertising the route to the next AS, the AS number is added to the beginning of the AS path. Each router stores the destination prefix with a single preferred BGP path. Compound policies are applied for the selection of a path, and the router makes a decision to advertise the path to neighboring routers in a different AS [Butler et al. (2010)]. The BGP routing system is not aware of a finer level of topology inside the local AS, or inside any remote AS.

3.2. RELATED WORK

In Path Diversity Aware Interdomain Routing [Wang and Gao (2010)] the authors have given an idea of path diversity that joins multiple path advertisements with path diversity to avoid routing interruption and to reduce packet loss because of routing failures. To increase the degree of path diversity existing in the underlying network infrastructure, the authors` approach allows routers to advertise an alternative path along with the best path. Therefore, the routers can take advantage of the diversity in paths, and they can find more alternative paths than that of what available in the existing approach. Having multiple paths, which are different from each other, help networks quickly recovery from failures. If a router has multiple paths to the same destination, it could quickly restore connectivity by switching to the alternate path when the main path becomes unavailable without waiting for exchanging announcements and withdraw messages from neighbor routers.

Today the existing interdomain routing system is one of the biggest systems which is a distributed in nature, and in such situation designing a scalable interdomain routing with the use of multiple path advertisement is very challenging. These challenges are like how much degree of path diversity is required to overcome network failures. Rather, considering the required cost to maintain multiple paths, one needs to understand when to send more paths to a router in order to perform a local recovery during failures. There are two rules for alternative
path advertisement, which help routers to decide when an alternative path should be advertised and when not to advertise. Hence, instead of blindly advertising alternative paths indiscriminately, routers use the intelligence by following two rules to send alternative paths to those neighbors, which will use those paths in the future to recover failures.

Figure 3.1(a) gives the overview of the conventional approach of an interdomain network, where five routers from router id 0 to 4 are connected together in the shown topology. Initially when all the routers come up, they only know their directly connected neighbors, and they exchange information with each other and subsequently each router come to know about other router's reachable destination prefix, but in case of BGP speaker routers, these routers only advertise their best path to a destination prefix.

The figure 3.1 (a) shows routers routing table information about only one destination prefix connected to router 0. The router 1 has path 1 0 to reach router 0, and it is it's best path, therefore router 1 advertises it's best path 1 0 to its neighbors router 2 and router 3. The router 2 and 3 use the path of router 1 and it becomes their best path therefore they also advertise it to
their neighbors, router 2 advertises its path 2 1 0 to router 3, and router 3 does the same to router 2 and router 4. But router 4 is on different side so it uses its direct path 4 0 to reach router 0. And router 4 advertises its best path 4 0 to its neighbor 3. Hence router 3 receives three paths to reach router 0. But router 3 selects 3 1 0 its best path to reach 0.

![Figure 3.1 (b) D-BGP](image)

The figure 3.1 (b) shows a different approach than the conventional one. Here the routers in the interdomain network not only advertise their best path but additional path along with the best path the additional path is for the use in case of best path failure. The additional path is known as the alternative path. This alternative path is used as a backup path and helps recovering from a link or node failure. One important feature of this alternative path is that it is relatively different from the best path, which reduces the chances of getting the failed path once again as it was the case in the normal case of BGP shown in figure 3.1(a).

But the advertisement of multiple paths to neighbors may increase the requirement of the space at the routers to hold the additional information; there are two rules to reduce the number of alternative paths to be advertised to a neighbor [Wang and Gao (2009)].
Rule 1: A router $u$ does not advertise its alternative path $Q_{alt}$ to a neighbor $v$ if

1. $u$ has $v$'s best path $P_v$, an alternative path $Q_v$, or both;

2. $|P_{best} \cap P_v| = 0$ OR $|P_{best} \cap Q_v| = 0$

Figure 3.2: Avoiding advertisement

In the network shown in figure 3.2, router of AS 4 checks condition 1 and then it refrain from advertising path 4 3 0 to router of AS 2. The AS path of a router represents the available paths in the router's routing table.

Rule 2: A router $u$ does not advertise its alternative path $Q_{alt}$ to a neighbor $v$ if

$$|P_{best} \cap Q_{alt}| < |Q_{alt} \cap P_v|$$

The rule 2 is applied on router in AS 4, a network shown in figure 3.3, there the router find that the rule 2 does not permit to advertise the alternative path 4 3 5 0 to the router in AS 2.
Figure 3.4, router 3 chooses path 3 1 0 as its best path so that router 1 will not know router 3’s best path. Suppose that router 3 has not advertised its alternative path 3 4 0 to router 1. Since router 1 does not have any path coming from router 3, router 1 advertises its alternative path 1 2 0 to router 3. When router 3 prepares to advertise path 3 4 0, router 3 finds that its best path 3 1 0 and the path 3 1 2 0 from router 1 share the link 3 1 (does not satisfy Rule 1), and the alternative path 3 4 0 is totally disjoint with all router 1’s paths (does not satisfy Condition 2). Thus, router 3 advertises the alternative path to router 1. After router 1 receives the alternate path, it realizes that router 3 can provide a disjoint alternative path so that router 1 does not need to advertise its alternative path 1 2 0 to router 3. Finally, router 1 sends a withdrawal to withdraw the path.

The D-BGP is modifying the way the BGP selects its best path. An alternative path is always inferior to the best paths, therefore the alternative paths is not used unless the best path fails. The reason behind this is that using an alternative path requires a control plane signaling to avoid possible forwarding loops. But in a situation when only alternative routes are left in a router’s routing table, then among the available alternative paths, the one with the shortest path
to the destination is installed as the best path. When an alternative path is selected as the best path, the router should send a withdrawal back to the sender of this alternative path as poison reverse.

This approach has complexity due to the message overhead for a failover event in D-BGP is bounded by $O(|E|)$, where $|E|$ is the number of links. After a node receives its first withdrawal/announcement, it will send out at most one withdrawal or announcement message to each neighbor. Thus, the message overhead is bounded by $O(|E|)$.

### 3.3. Issues of BGP

BGP is susceptible to the weaknesses of the interdomain routing environment [Israr et al. (2009)].
a) It does not have any mechanism to check the integrity, freshness and source authenticity of BGP messages. BGP does not have any mechanism for the verification of authenticity of an address prefix and also an AS origination of the prefix in the routing system.

b) The BGP protocol does not guarantee the correctness of the attributes of a BGP UPDATE message [Israr et al. (2009)]. BGP routing events occur very often and the routing behavior of BGP during route convergence has not been understood.

c) Only very little is known about how the route dynamics cause the degradation of end-to-end performance, or about the impact of topological properties, routing policies, and routing configurations on routing behavior.

d) Routing loops cause packet loss and packet delays as packets are caught in a loop. BGP experiences transient routing loops and also transient loss of reachability due to route convergence.

e) A router experiences transient loss of reachability during path exploration in the route convergence process due to limited route visibility. Packet losses are caused due to transient routing failures [Wang and Gao (2009)].

f) The growing complexity of BGP has led to configuration errors, software bugs, slow convergence, risks of persistent route oscillations, security vulnerabilities, economically-driven manipulations, and mismatches between the AS-PATH and the path data traffic actually travels [Schapira et al. (2010)].

g) The failure of a link(s) or node(s) has severe consequences on interdomain routers as it may cause the loss of hundreds of packets in transit, and the resetting of connections [Kumar and Kumar (2009)].
h) A coordinating mechanism to facilitate diversified or determined interdomain routing is not available in the BGP. The BGP guarantees reachability but no routing versatilities. Deployments of routing functions such as QoS and multicast are difficult in interdomain scenarios.

3.4. Problem Identification & Proposed Solution

D-BGP [Wang and Gao (2009)] allows a BGP router to select the most disjoint alternative path in case of a route failure. If there are multiple alternative paths available, the shortest path is taken as the best path. However, D-BGP does not consider the characteristics of that selected path such as, link and bandwidth availability. The selected best alternative path may be different from the previously selected best path in terms of having different intermediate nodes, but if this path is already experiencing congestion (the available bandwidth on this path is very low), then it may also result in failure. In D-BGP, update messages are propagated for both the best path and alternate path, thereby increasing message overhead.

To overcome the above mentioned problems, this chapter proposes a design for a robust BGP protocol that is fault tolerant and reduces message overhead. The proposed protocol uses D-BGP for alternate path selection. Here D-BGP selects the shortest path as the alternate path between the BGP speaker and BGP peer. The alternate path selection is based not only on the number of hops between the BGP peers but also on bandwidth availability and link availability, so that the alternate path is failure free. Estimation of available bandwidth and delay is obtained from the abstract link (at the Data Link layer), which maintains connections between different Autonomous Systems, as the BGP itself does not maintain any such information. The proposed protocol collects information from all intermediate links and considers minimal data in case of bandwidth and maximal in case of delay.
The proposed protocol utilizes PED [Huston et al. (2010)] for delaying the update messages for both the best path and alternate path. A path longer than the previously existing path between the BGP speaker and the BGP peer is known as a longer path. If the update message is sent from the BGP speaker to a BGP peer through a path longer than the existing alternate path, it is delayed, and for the shortest paths, the update messages are readily sent to the peer.

3.5. Fault-Tolerant Robust BGP Routing Protocol

The interdomain routing protocol requires each interdomain speaker router to advertise its best path to all the BGP speaker routers to which it is directly connected. When a failure occurs, the speaker router must select an alternative path to survive the failure. However, it is not known whether the alternative paths available to this router are relatively good or bad. If the alternative path selection is relatively bad, it may lead to a worse routing scenario and may cause loss of reachability to other prefixes also. The routing system design is proposed to minimize the chances of failure for an alternative path after the failure of the previously known best path.

3.6 Diversity-Aware Interdomain Routing

In diversity-aware interdomain routing, each interdomain router selects routes that have the fewest intermediate routers common to the existing best path. In this manner, the failed node will not be a part of the newly selected path.

The D-BGP selects and advertises the alternative paths, and reacts to the failure of a single link or node. Initially it advertises multiple paths and selects the best path and alternative paths. The D-BGP computes disjoint paths by comparing all the available paths with the currently installed best path, and the path that has the fewest common entries is selected.
3.6.1 ADVERTISING MULTIPLE PATHS

The best path and alternative path are identified using path identifiers in D-BGP. The appropriate routes should be exported before sending out an alternative path. The routing policies and the alternative path advertisement rules are surpassed by the alternative path. If the best path is the only path sent to the neighbor, the best path is advertised by the router.

For instance, advertisement of a best path from a router is not sent to the neighbor from whom it was learned. When only the alternative path is sent, a new update message with an empty best path is generated by the router and is attached to the alternative path. This message is sent to the neighbor. A withdrawal message is sent to the router when the best path and the alternative path are not allowed.

When paths are not available, the router withdraws the previously announced best path or alternative path. The changes in the router are sent to every neighbor by sending a Root Cause Notification (RCN) along with the triggered withdrawal. To specify the unavailable paths, withdrawals use path identifiers. In some cases, although paths are available the router may withdraw previously announced alternative paths. The neighbor that provides a path disjoint with the router’s best path, does not receive the advertisement of the alternative path from the router.

Prior to learning of the disjoint path, the router is capable of sending out the alternative path that is due to the path propagation delay. When the router receives disjoint path, the router recognizes that the alternative paths should not have been sent. Then, a withdrawal with the alternative path identifier will be forwarded to withdraw the path [Wang and Gao (2009)].

3.6.2 SELECTION OF BEST PATH AND ALTERNATIVE PATH

By definition, alternative paths are of lower grade than the best paths. When the best path is available, the alternative paths are not used. This is due to the reason that, the forwarding of the
loops is avoided by using control plane signaling in the alternative routes. Among the alternative routes in the routing table, the best path installed is the one with the shortest path to the destination.

Withdrawal of the alternative path is sent to the sender as a poison reverse while selecting the alternative path as the best path. With respect to path disjointedness in D-BGP, the router selects an alternative path among all available paths. The path most disjoint with the router’s best path should be selected as the alternative path [Wang and Gao (2009)].

During path selection, to obtain a failure free alternative path, the delay metric and bandwidth availability are considered. The available bandwidth is a measure of the residual available bandwidth of the link.

3.7 SCALABLE BGP LINK STATE (SBLS) ROUTING FOR DELAY METRIC

In this section, a scalable BGP link state routing using link state protocols is proposed that supports interdomain traffic engineering (TE).

The abstract link \( l \in L \): Several available paths between two Border routers in the domain’s abstract topology.

The delay metric is calculated to monitor and advertise the link status. The delay of a path is the sum of the delay metrics of all links along the path.

Here \( R(l) \) is defined as the delay of the link \( l \) and \( R(P) \) to be the delay of path \( P \). Then

\[
R(P) = \sum_{l \in P} R(l) \quad \text{................ (3.1)}
\]
Where $\eta$ is the set of all links in $P$. An upper bound $U_l$ is set for each abstract link $l$ in the domain.

The TE attribute aggregation considers only the paths whose delay is not larger than $U_l$.

The paths that carry interdomain traffic are restricted by the abstract link’s metric. For paths that do not satisfy $U_l$, the traffic flow is rejected because it may violate the service requirements of the user, or break the traffic regulation of the domain’s operator.

Thus the path that has a shorter delay is considered for alternative path selection. The set of paths between border routers $x$ and $y$ satisfying the upper bound of delay is:

$$S_{(x,y)} = \{ A | A \in S^{r}_{(m,n)} , R(A) \leq U_l \}$$

Here $S^{r}_{(m,n)}$ denotes the set of all possible paths between BGP routers $x$ and $y$.

The delays of paths that are taken into the aggregation should be below the $U_l$ of its corresponding abstract links [Wang et al. (2009)].

### 3.8 Scalable BGP Link State (SBLS) Routing for Available Bandwidth

The available bandwidth of a path is determined by the physical link with the minimum available bandwidth along the path. For link $l$, let the bandwidth be $w(l)$, the bottleneck link of path $A$ be $l_{B(A)}$, and the bandwidth of path $A$ be $w(A)$.

$$w(A) = \min_{l \in E_{A}} w(l) = w(l_{B(A)})$$

................. (3.3)
Using the bandwidths of paths in $S_{(x,y)}$, it is possible to determine the bandwidth of an abstract link $U_l$. A single routing path can be routed without loss of generality.

The aggregated bandwidth attribute of abstract link $U_l$ is defined to be the maximum bandwidth of all paths in $S_{(x,y)}$.

A larger upper bound metric represents the cost or the domain’s unwillingness to carry traffic with a larger bandwidth. If $w(A)$ exceeds $U_l$, it is possible to find paths with the maximum available bandwidth and these can be used as alternative paths in case of failures [Yu et al. (2009)].

3.9 LINK MONITORING AND ADVERTISING

This technique can select a set of bottleneck links to monitor in paths in $(x,y)$. According to equation (3.3), the maximum bandwidth of monitored links is taken as the bandwidth of their abstract links.

Let $E^K_{(x,y)}$ denote the set of monitored physical links for abstract link $U_l$. The bandwidth of $U_l$ is obtained as

$$w(U_l) = \max_{l \in E^K_{(x,y)}} w(l) \quad \ldots \ldots \quad (3.4)$$

Thus, the states of individual abstract links can be identified. Changes in the bandwidths of monitored links will trigger state computation and advertising for $U_l$. It is feasible to advertise its state individually. Additionally, this scheme reduces the computational complexity of TE information aggregation by comparing the bandwidths of only monitored links rather than computing the bandwidth of each monitored path [Yu et al. (2009)].
3.10 PATH EXPLORATION DAMPING (PED)

To improve the BGP convergence time, the update messages for both the best path and the alternate path are delayed subject to some worst case scenario. Path Exploration Damping (PED) is used to suppress BGP’s protocol behavior when BGP undertakes certain forms of “path exploration”.

The announcements of certain routes are restrained by PED using a timer, and the update suppression selection algorithm related with AS path attribute behavior is used. The other updates and withdrawals propagating through a BGP’s speaker are not delayed. Compared to existing damping mechanisms with PED, the volume of BGP update message is reduced. The BGP speaker will not incur undue additional overhead [Wang and Gao (2009)].

The alternative paths have been calculated based upon delay, hops in the path, and bandwidth. Paths are classified as longer and shorter, depending upon the number of hops. Bandwidth is classified as lower and higher using the upper bound as described earlier. Delay is differentiated into shorter and longer using the upper bound. The worst case and best case scenarios are determined based on the combinations (CB) given below:

When selecting an alternative path, a worst case scenario consists of

(i) Longer path (LP)
(ii) Longer delay (LD)
(iii) Lower bandwidth (LB)

So the CB for a worst case scenario is \{LP, LD, LB\}

A best case scenario consists of

(i) Shorter path (SP)
(ii) Shorter delay (SD)

(iii) Higher bandwidth (HB)

So the CB for a best case scenario is \{SP, SD, HB\}

When an alternative path with the worst case scenario is discovered, the update message of that path is delayed using PED. For the best case scenario path, the update messages are sent immediately. The algorithm mentioned below describes the actions taken for worst case and best case scenarios by setting a timer in the new path.

Table 3.1: Algorithm for robust BGP

<table>
<thead>
<tr>
<th>Algorithm : Proposed fault tolerant robust BGP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Set new path exploration damping interval (PEDI) timer</td>
</tr>
<tr>
<td>2. If worst case CB for alternative path</td>
</tr>
<tr>
<td>Then</td>
</tr>
<tr>
<td>2.1 If PEDI timer is inactive</td>
</tr>
<tr>
<td>Then</td>
</tr>
<tr>
<td>2.1.1 Queue the update &amp; start timer</td>
</tr>
<tr>
<td>2.2 Else</td>
</tr>
<tr>
<td>2.2.1 Remove previously queued updates for CB</td>
</tr>
<tr>
<td>2.2.2 Queue new update</td>
</tr>
<tr>
<td>2.2.3 Restart PEDI timer</td>
</tr>
<tr>
<td>End If</td>
</tr>
<tr>
<td>3 Else If best case CB for alternative path</td>
</tr>
<tr>
<td>Then</td>
</tr>
<tr>
<td>3.1 Remove previously queued updates for CB</td>
</tr>
</tbody>
</table>
3.2 Send new update
End If
End If

4 If candidate update is detected
Then
4.1 Extend the damping period of PED
End If

3.11. SIMULATION RESULTS

This section describes the simulation and reports its results obtained. Figure 3.5 shows the simulation topological structure of the interdomain speaker routers, with each node representing an autonomous system.

Figure 3.5: Simulation Topology
3.11.1 SIMULATION SETUP

The Network Simulator (NS2) has been used [ns-2 (2008)] for the experimental setup and performance evaluation of the proposed algorithms. NS2 is a general-purpose simulation tool that provides discrete event simulations of user defined networks. The proposed Fault-Tolerant and Robust BGP (FTR-BGP) routing protocol is compared with the D-BGP protocol. The ns-BGP extension 2.0 for ns-2.33 [ns-BGP (2008)] is used to simulate the BGP architecture. The simulation topology is shown in Figure 3.5. In simulation topology 11 ASs are connected to each other. The network prefix addresses for each AS range from 1x.0.0.1 to 1x.0.10.1. The link bandwidth is 10 Mb and the link delay is 20 ms. BGP agents are attached to all AS nodes. CBR traffic is used with a packet size of 100 bytes. The traffic rate is varied from 1.5 Mb to 5.5 Mb. The CBR traffic flow is initiated from the source AS9 to the destination AS3. Initially, traffic takes the optimum path AS9-AS0-AS1-AS2-AS3. At 2.2 seconds, the link AS0-AS1 breaks due to link failure and the alternate path with good link quality and bandwidth is taken by the proposed FTR-BGP protocol as AS9-AS0-AS11-AS1-AS2-AS3.

3.11.2 SIMULATION RESULTS

Simulation results are displayed in figures 3.6 to 3.11.

BASED ON RATE

In the first simulation, the traffic sending rate is varied from 1.5 Mb to 5.5 Mb. Packet loss, end-to-end delay and received bandwidth are measured.

Figure 3.6 shows that the Received Bandwidth increases whenever the sending rate increases. From the figure, it is evident that FTR-BGP has a higher received bandwidth compared to D-
BGP. In figure 3.7, it is observed that the delay of FTR-BGP is lower than that of D-BGP. Figure 3.8 shows dropped packets for both protocols. Packets dropped by FTR-BGP are very low when compared with D-BGP.
BASED ON TIME INTERVALS

In the second simulation, the performance is measured at various time intervals during the simulation. The interval is fixed at 0.5 seconds and varied from 1 to 10 seconds.

From figure 3.9 shows the Received Bandwidth of both protocols. Because there is a link break at 2.2 seconds, there is no flow from 2.2 to 5.5 seconds for D-BGP until the link failure is recovered. However, because FTR-BGP immediately takes the alternate path, the received bandwidth is constant after 2.5 seconds.

In figure 3.10, it is observed that the delay of the proposed FTR-BGP starts decreasing at 2.5 seconds, whereas in D-BGP the delay begins to increase at 2.5 seconds and begins to decrease only at 6 seconds. FTR-BGP experiences higher delay initially due to the computational overhead required to obtain the link availabilities and bandwidth. This is due to the fact that the D-BGP tries to recover the failure during that time. From figure 3.11, after failure when traffic is monitored, it is evident that the number of packets dropped by FTR-BGP is very low when compared with D-BGP.

Figure 3.9: Time vs. Bandwidth
This chapter proposes a fault tolerant robust BGP protocol that is based on the quality of the path and reduces BGP route update-message overhead. The proposed protocol uses D-BGP for alternate path selection. Scalable BGP link state routing has been proposed for calculating the link availability and bandwidth availability. Link availability is based on the delay metric. An upper bound is selected for delay and lower bound for bandwidth, the path that satisfies the criteria is selected as the alternative path. Update messages are delayed for those alternate paths with worst case distance, delay and bandwidth. A path exploration damping interval (PEDI) timer is utilized for delaying the update messages. Simulation results show that the proposed FTR-BGP routing protocol performs better in terms of higher available bandwidth, 3.12. CONCLUSIONS
minimum delay, and minimum packet drop. Therefore it is failure free in the internet environment.

However, there are some challenges in this work. After the failure of a previously selected best path computational overhead is incurred for calculating the bandwidth and link availability in selecting an alternative best path. From figure 3.10 it is evident that the initial delay is high when the alternate path is selected. Traffic will increase on that selected path, which may affect traffic conditions on that path. Efforts may be made to overcome these limitations in the future.