A Proactive Component for a Fast Emergency Paths Schema to Bypass Failures in IP Networks

Fernando Barreto
Federal Technological University of Paraná
55 41 3310-4679
fbarreto@cpgei.cefetpr.br

Luiz Nacamura Junior
Federal Technological University of Paraná
55 41 3310-4679
nacamura@dainf.cefetpr.br

Lúcia Valéria R. de Arruda
Federal Technological University of Paraná
55 41 3310-4679
arruda@cpgei.cefetpr.br

ABSTRACT
The increase of the Internet dependency to support general services and real time services has generated a need for a more reliable IP network. In case of transient failures, the routing protocols are not as effective in obtaining a new route, since they take several seconds to converge. During this time, instability occurs of wrong packet forwarding process, causing high packet loss rates and thus compromising the quality of network reliability. This study proposes a proactive calculation approach for emergency paths to be available in case of transient failures, which would generate few changes in the functioning of the IP routing algorithm. Such an approach makes these paths available directly on the router’s forwarding information base to be promptly utilized as soon as a failure is detected, allowing for reduction of packet losses.

Categories and Subject Descriptors
C.2.2 [Computer-Communications Networks]: Network Protocols – routing protocol

General Terms
Performance, Reliability, Heuristic.

Keywords
Routing, Reliability, Failure, Fast Rerouting, IP.

1. INTRODUCTION
The Internet is becoming a huge infra-structure for exchanging critical information, from simple person applications, such as e-mail and web pages, to business applications, such as electronic commerce, bank transactions and VoIP. The information traffic dependence on the Internet is causing an increase of research for robust and reliable IP networks to support possible configuration changes in network state.

A robust and reliable IP network is able to sustain traffic flows even when a failure occurs changing the network infra-structure. Once a problem has been detected, the network must adjust the damaged traffic flows trying to influence as little as possible their performance. The objective here is achieving high connectivity to support all the flows.

Unfortunately, the failure problems are frequently found in day-to-day network operations. The link or router, i.e. node, failure existence is resulted of many events such as: node software maintenance, network interfaces failure, an accidental fiber rupture and Shared Risk Link Group (SRLG) rupture.

At the actually IP networks, the network components failure inside a domain are handled by the link state routing protocols Interior Gateway Protocols (IGP) such as Open Shortest Path First (OSPF) and Intermediary System to Intermediary System (IS-IS).

When these protocols detect an adjacent failure in a node, they first start a contention time period allowing a possible physical layer correction for the failure. If this contention time expires, the routing protocol routine in this node reacts to the failure informing all the other topology nodes within its domain about the link state change. This forces all the nodes to recalculate their shortest path tree using Shortest Path First (SPF) algorithm [8] and update their Routing Information Base (RIB) and Forwarding Information Base (FIB).

This entire reactive process needs an execution time enclosing all the network nodes. It is called convergence period. The end of this period occurs when all the nodes update their RIBs and FIBs according to the new network link state that fits this failure. This period of time may vary from one topology to another, because the network topology diameter, number of routes affected, RIB and FIB updating, congestion, link speed and a lot of other factors directly influence the amount of time necessary to execute this process [4].

Recent research has shown that the time spent from failure detection until the end of the conversion time period varies from a few seconds to tens of seconds [10][2] and, in the worst case, even tens of minutes [5]. During this time, instability occurs with RIB and FIB information in the nodes, which results in wrong packet forwarding and may cause routing loops, packet loss with incomplete FIB information and inaccessible destination networks. For example, if an OC-192 (9.6Gbps) link is down for ten seconds, assuming an average packet size of 1KB, close to 46 million packets are lost. This high packet loss rate affects seriously any TCP application and damages any real time application.

Recent research has divulged a survey about backbone failure characteristics in IP networks, and about 50% of failures are transient and they usually last less than 1 minute [11] [13]. In addition, the occurrence of a failure is more common than multiple simultaneous failures [17]. When there is a fast network state change caused by the transient failure characteristic, there is the possibility of two convergence periods for each link state change, which generates a sum of these two instability periods.
very close to each other making the network environment more unstable.

In face of these transient failure problems, there is a necessity for Traffic Engineering (TE) solutions [3] to suppress the routing protocols, optimizing and controlling the data performance flows (packet delay, packet loss rate, jitter and throughput) and also optimizing the utilization of resources. Among the TE objectives are the congestion reduction, efficient use of available resource and achievement of Quality of Services (QoS) for some applications.

In Multi-Protocol Label Switching (MPLS) networks, the TE processes that handle the failures in a fast way are named Fast Reroute [22]. This mechanism is designed to bypass a detected failure at local scope, once it is activated by the failure detecting node using a pre-calculated and a pre-signaled repair path, named Label Switch Path (LSP). There are two techniques to manage these paths: splicing and stacking. The splicing technique constitutes a LSP originated in the detecting node and extended until the original LSP destination node affected by the failure. This technique needs a lot of resources due to the excessive number of recover LSP, that is, one for each original LSP, and for this reason, it is not scalable in large networks. The stacking technique creates paths that bypass the failure and end in the next node after the failure, along the original LSP sequence. The deviated flows are encapsulated to follow this LSP recover. Among the problems of this last technique is the global label distribution allowing the LSP recover end node knows which LSP the deencapsulated packet must follow. Another problem is the encapsulated packet, because the packets may exceed the Maximum Transfer Unit (MTU), and if it occurs there may be a need to discard the packets [28].

In case of IP networks, this TE process previously computes alternative routes allowing an immediate recover from a failure without informing other nodes about the change in network link state [18]. This mechanism is very similar to MPLS approach, but it does not need all the necessary virtual circuit infra-structure to make MPLS available.

In general, the TE processes are either proactive or reactive, and either local or global. The proactive processes are those which realize calculations and necessary routines to make TE solution before failure occurs. The reactive processes realize the path calculations and necessary routines after failure occurs. Considering the failure recover scope, a TE process can be local – performing at the node closest to the failure and this node is then responsible for redistribute the affected flows. At the global recover scope, it is left to special nodes, generally the topology border nodes, which must be signaled by the failure detector node, to reorganize the affected flows.

This approach is oriented to IP networks and, for these authors, the most suitable TE processes for transient failure problems are the proactive and the local processes. One reason is that they offer an immediate solution to be performed by the failure detector node, and it does not need to have signalization to network border nodes.

Some approaches with TE processes for IP networks try to follow some of these characteristics reorganizing the affected flows. Table 1 presents theses approaches.

| Approach | (Reactive | Proactive) (Link | Node Failure) | Objectives |
|----------|-------------|-----------------|------------|
| [19]     | Reactive, Link e Node | Bypass the failures and congestions finding paths from exchanging information among its neighbors. | Drawbacks: only reactive. |
| [15]     | Reactive, Link | Reactive approach to find a alternate path restricting the link state information to some nodes pertaining to this alternate path. | Drawbacks: only reactive working only with link failures. |
| [17]     | Reactive, Link | A Tabu Search heuristic to find the link weights bypassing link failures obtaining multiple paths with ECMP. | Drawbacks: works only for link failure and still flood link state information to all nodes. |
| [16]     | Proactive, Link | Local rerouting with FIB’s forwarding in each network interface fulfilled from a failures deduction. | Drawbacks: works only for link failures and can generate routing loops. |
| [20]     | Proactive, Link and Node | Improves [16] approach getting FIBs for each interface having routes to bypass node deduction failures. | Drawbacks: FIB for each interface and a modified SPF considering FIB’s forwarding |
| [1]      | Proactive, Link and Node | Provide link weights rules to obtain loop free alternate (LFA) paths. | Drawbacks: doesn’t achieve 100% of failure cover and depends on link weights values. |
| [6]      | Proactive, Link and Node | Routes to not-via addressing used to encapsulate compromised flows respectively to one particular component. | Drawbacks: encapsulation technique and additional used network resources. |
| [24]     | Proactive, Link and Node | Making various sub-topologies each one bypassing failures, maintaining a RIB and a FIB for each of these sub-topologies. | Drawbacks: use of various RIB and FIB, may creating more long paths than [6] approach. |
In this context, the present article proposes a new proactive approach to calculate emergency paths for the Fast Emergency Paths project.

2. FAST EMERGENCY PATHS (FEP)

The OSPF routing protocol realizes a rerouting which cannot be entirely classified either as global or local. It acts in a reactive and distributed way efficiently adapting to any change in the network topology. However, efficiency does not reach changes caused by transient failures, because it never provides recovery in a time-scale suitable for this kind of failure. In [9]’s view as well as in our own, among the approaches checked, which offer some fast rerouting mechanism and path 100% covered, is the not-via [6] approach. This approach obtains high reliability, but without considering a good policy for resource use. As a consequence, it develops paths that make excessive use of resources to repair a failure. Another problem is the encapsulation technique used, because there may be situations which exceed the packet MTU limit. When this situation occurs in IPv4 networks, fragmentation is necessary, and in IPv6 networks it must discard the packets.

Taking into consideration these problems, the proposal in this study is to investigate a local recovery path similar in some aspects to the approach [6]. This emergency alternative path obtained is also expected to offer 100% network cover, avoiding failures. Though, it should not choose paths which are longer than necessary.

This article presents a proactive recovery path calculation which consists of a TE schema component for fast, local and distributed rerouting so called Fast Emergency Paths (FEP) [23]. The main objective of the FEP schema is to attain high network connectivity in order to maintain the backbone reliability, a feature of that is becoming more and more fundamental for the passing traffic flows.

FEP proactive approach, also called FEP_proactive, constitutes a heuristic which generates various recovery paths, named emergency paths, which are available to allow the forwarding of the passing traffic flows that have been affected by a failure. Bypass is the main characteristic of these paths in order to avoid either a node or a failure link. Their shape can, thus, be selected by verifying the contour possibilities.

2.1 Necessary Conditions for FEP_proactive

According to these authors, the first necessary condition for FEP_proactive – and also for any IP fast rerouting approach – is the existence of a physical structure of the backbone topology able to support, at any point of the network, at least one failure, either node or link. In line with graph’s theory, in formal terms, the nodes of a network topology are represented as the vertices, and the links, as the edges connecting two vertices, with their non-negative costs, in a bidirectional shape. In order to have a graph of any kind able to support vertex failure and, at the same time, maintain the connectivity among all the vertices, better saying, that an alternative path still exists to connect every two vertices of a graph, it is necessary that a graph be $k$-connected [7]. The variable $k$ indicates the removal of $k-1$ vertices from the topology and that yet it maintains the connectivity among all the nodes. Therefore, a minimum topology is to be at least 2-connected, i.e., with $k=2$ indicating a graph able to support total connectivity among the vertices, even removing the maximum of (2-1) vertices from the graph.

As observed in [17], it is reasonable considering failure of a single network component, since multiple simultaneous failures are rare in real backbone topologies and an additional complexity, including approaches which comprise multiple failures, is undesirable.

The second necessary condition is related to the network planning, which must be engineered with the goal of keeping the load level of every link under 50% in the absence of a failure [11]. The objective is to allow an accommodation of traffic deviated due to a failure.

In the authors’ view, the specification of the link weights is an offline TE approach to accommodate a determined traffic flow matrix by means of OSPF shortest path paradigm. In doing so, there are several research works which seek to exhaustion in a range of solutions the best weight distribution for the links. Two examples are [21] and [17]. Hence, FEP_proactive develops a heuristic which is independent of the link weights planned to a single OSPF area by any of these approaches. The objective here is to provide only emergency paths which serves to bypass failures and are available to be used when needed.

Considering a topology of at least 2-connected, and with traffic distribution limited to < 50% of links utilization capacity, employing FEP_proactive to obtain recovery paths seems feasible.

2.2 FEP_proactive Functioning

Each node in a backbone network topology has internal components which manage the node functioning, either in terms of routes and forwarding. These components are the following: the routing protocols and the forwarding routines.

The link state routing protocols implement the routing algorithms responsible for calculating RIB based on approaches such as metric, hop count, link capacity, etc. The most largely used algorithm is the OSPF [12] and, for this reason, its use has been adopted in this study. An extension of this work to other link state routing protocols can be easily adaptable. The algorithm of the OSPF executed in each node is the SPF [8] and uses the link weights as metric in order to calculate a shortest cost path from its node to another along the topology in which the OSPF is acting. After the calculation of the shortest paths, the RIB is fulfilled by the identification of routes for each destination network informed by the link state messages from each node. Once fulfilled the RIB, the FIB fulfilling proceeds, which is used by the forwarding routines in order to accomplish the task of forwarding packages through the node.

The forwarding routines deal with fast packets processing, and realize a IP header examination, searching for a FIB entrance with results in a active network interface for each packet analyzed. With this information, the analyzed packet is queued on the respective active network interface queue so that the packet can be processed.

The FEP_proactive is executed on each node of the topology and on the scope of the routing algorithm, that way, adding a new
module with an algorithm named VectorSPF, which works together with the OSPF routines for the calculation of emergency paths. The VectorSPF utilizes the database from the shortest paths, calculated by the OSPF, and acts upon this base simulating the removal of each network component adjacent to this node. It could be one node together with the link or just the link. For each component removed, a new SPF calculation is done for all the destination nodes affected by the failure in the SPF tree. An alternative path is generated to bypass the supposed component in case of failure.

Besides this alternative path, an intersection is realized between the original path, generated by the OSPF, and the alternative path, generated by the VectorSPF, seeking from the source node to the first node at the points these two paths meet. The result is an emergency path, which follows the alternative path avoiding the simulated component with failure and ending at the point it reaches the shortest original path. This emergency path is fulfilled at the FIB with an additional field in the shape of vector, which represents one VectorSPF of the shortest emergency path nodes.

This emergency path must necessarily meet the shortest emergency path, at least, in the worst case, the destination node. In this case, the two paths are disconnected and the only points they have in common are the source and destination nodes. In other cases, the emergency path must find the original path in some node, which is here named q. From q, the packets must follow their original routes without routing loops. To prove this affirmation, we present an adapted property from the theory of shortest-path tree [29].

**Property 2.2.1.** Considering the subpaths from s to q, with distance d(s,q), and from q to k, with distance d(q,k), which belong to a shorter path from s to k, these subpaths are consequently a shortest path between the origin vertex and destination vertex of each one of their subpaths, i.e. from s to q and from q to k.

The basic idea of this property derives from Bellman's inequalities [30], which govern the problems of shortest-paths. Let G=(V,E) be a graph in which each edge (i,j):E is weighted by a nonegative cost c_{ij}. For any two vertices u and v, let d(u,v) be the distance of the shortest path in G from u to v.

1. If (s = v_0, v_1, ..., v_t = t) is a shortest path from s to t, then the subpath (v_i, v_{i+1}, ..., v_j) is a shortest path from v_i to v_j.
2. For all edge (u,v) ∈ E, we have d(s,v) ≤ d(s,u) + c_{uv} with d(s,s) = 0.
3. The path (s = v_0, v_1, ..., v_t = t) is a shortest path from s to t if and only if
   \[ d(s,v_i) = \min_j \{ d(s,v_j) + c_{v_j,v_i} \} \]
   for i=1,...,t.

After the end point of the emergency path, the packets are able to follow their paths until t – from q – without causing routing loops. This happens because the path q to t belongs to the shortest original path from s to t and, therefore, it is the shortest path from q to t. This statement fits the description of Bellman's inequalities.

In this sense, the emergency path serves to avoid routing loops, and it extends only the necessary to cover the failure, which does not happen with [6].

For the decision on which component, node or adjacent link, should be removed in order to calculate the VectorSPF, it is verified when the topology destination node of a network prefix is located at the adjacent node. In this case, the link should be selected to be bypassed since the adjacent node is already the end of the shortest original path and could not, therefore, be avoided.

The following example illustrates a situation in which the nodes b, j and k simulates a failure in the node h generated by the VectorSPF in each node b, j and k.

![Figure 1. Example of a simulated failure.](Image 320x478 to 555x586)

The topology illustrated in Figure 1 presents a failure in node h and reveals that the nodes b, j and k would not have enough and immediate information to identify the kind of the detected failure: link or node adjacent to link. This uncertainty leads preferable to a calculation of the emergency path always in order to avoid the adjacent node. Otherwise, in case the adjacent node is the destination node of a shorter original path, the emergency path is then calculated in order to avoid the adjacent link to this node only. Table 2 illustrates how part of the node b FIB looks to the destination networks affected by the component with failure, as simulated, either b-h link or h node. One representation similar to this Table 2 occurs with the nodes j and k, which also attempt to avoid the simulated failure.

<table>
<thead>
<tr>
<th>Table 2. FIB at node b</th>
</tr>
</thead>
<tbody>
<tr>
<td>dest.</td>
</tr>
<tr>
<td>dest. e, next node h</td>
</tr>
<tr>
<td>dest. g, next node h</td>
</tr>
<tr>
<td>dest. k, next node h</td>
</tr>
</tbody>
</table>

It can be observed that the FIB has just a simple information addition, which does not interfere in the original OSPF functioning. The destination networks presented (destination e,g,k,h) are simply illustrative indicating that any destination network prefix announced by these nodes would use the same VectorSPF found. Such reutilization of the emergency paths reduces considerably the calculations for the amount of destination nodes and not for the amount of destination network prefixes affected by a failure, as reported in [26].
These VectorsSPF presented serve to assist the decision of the forwarding routine at this node in case a failure is detected, in order to avoid either the node $h$ or the link $b-h$ according to the destination node in question. The Table 2 three first lines show node $h$ being bypassed because the destination nodes do not identify the node $h$ as the last node of the shortest original path. Yet, the last line shows the result of a calculation of VectorSPF which avoids just the link $b-h$ because the last node of the shortest path to the destination node, identified by node $h$, is at the node adjacent to node $b$.

### 2.3 FEP_proactive Accuracy

FEP_proactive aims to find and make paths available in case there is a single failure in the topology, either in the node or in the link. These paths are developed by means of emergency paths calculation at local and distributed scope in order to help unstable network environments caused during a transient failure period.

The use of a specified path at the VectorSPF guarantees that routing loops are avoided, since the emergency path finds the original path calculated by OSPF in a region located after the failure, be it a node or a link. When it finds the shortest OSPF original path, the packet is able to follow its shortest path normally until the destination node.

Once the emergency path has the same cost as the original shortest path, then this emergency path can be easily used through ECMP. Yet, if the emergency path follows the LFA [1] restrictions, then it can be easily used redirecting the flow packets to it. These two particular situations allow the use of the emergency path without any risk of routing loop. Otherwise, a signaling approach should be used to guarantee a path without routing loop until the end node of the emergency path. After this node, the packets are developed to follow their paths without the occurrence of a routing loop, as observed in the Property 2.2.1 in Section 2.1.

One advantage of the VectorSPF in relation to the approach [6] is that when it finds the shortest OSPF original path, it immediately ends the failure bypass process, while the not-via approach does the opposite: it uses an emergency path until the failure surroundings, employing additional resources and, in some cases, drawing paths which are longer than the necessary. For illustrative purposes, still based on Figure 1, the not-via approach bypasses the failure encapsulating the $b\rightarrow e$ and $b\rightarrow g$ flow packets to a destination not-via $h$ address located in node $j$, following a path that ends in node $j$. From $j$, these packet flows follow the shortest path and, in the sequence, they follow to node $g$. In this case, one additional hop has been used in order to reach node $g$, and two additional hops have been used in order to reach node $e$.

If using FEP_proactive, the emergency path stretches only until node $g$, i.e. meeting point between alternative path and the original SPF path. Table 3 presents this comparison indicating in brackets the bypass path generated. What is outside the brackets indicates a return to the original path, when the bypass is no longer necessary.

### 2.4 FEP_proactive Heuristic

FEP_proactive generic algorithm, shown in Figure 2, should be run together with the routing algorithms in each node of an OSPF domain. This algorithm runs in a proactive approach and the treated failures are simply simulations, that is, they still do not exist. The shortest original paths generated by the OSPF in the routing algorithm are then reutilized. In each node of the topology, the following algorithm should be added together with the routing algorithm:

#### Table 3. Comparison between Not-Via x FEP_proactive paths

<table>
<thead>
<tr>
<th>Not-Via</th>
<th>OSPF + VectorSPF</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(b,d,h,j),g,e$</td>
<td>$(b,d,g),e$</td>
</tr>
<tr>
<td>$(b,d,g),j,g$</td>
<td>$(b,d,g)$</td>
</tr>
<tr>
<td>$(b,k)$</td>
<td>$(b,k)$</td>
</tr>
<tr>
<td>$(b,k,h)$</td>
<td>$(b,k,h)$</td>
</tr>
</tbody>
</table>

The algorithm to calculate the emergency path sketch, i.e. the alternative path, is the IncrementalSPF. This algorithm has a shorter running time than the original SPF, based on the principle that small changes, such as link or node failures, influence only a small part of the SPF tree. Therefore, it should be faster if the SPF calculations are done only in those parts of the tree which contain failure. In the worst case, the IncrementalSPF is as complex as the SPF, i.e. $n \cdot \log(n)$ which constitutes an improved version, or $O(n^2)$ which is the traditional version. For further details on IncrementalSPF, refer to [14] and [15].

#### Figure 2. FEP_proactive algorithm

In step 1, each active network interface of the node is identified. It is important to notice that an active interface is a point of connection in an interface card line, for example a fiber port, and an interface card line can provide various active interface points. In step 2, for each active interface verified the shortest paths should be found which would be affected by a failure in this active interface, identifying the destination nodes affected. The
calculation of the alternative path used is the IncrementalSPF suppressing the link and the adjacent node from the topology in steps 3 and 4, respectively. It is necessary to generate these two calculations in order to have VectorsSPF which encompass all the compromised SPF paths, that means, which guarantee 100% cover.

Step 5 allows a calculation of the VectorsSPF for each destination node of the affected SPF paths by the simulated failure. In generating this calculation, it is identified in step 6 the component to be bypassed., i.e. link or node, being a link in case the adjacent node is the destination node of the original SPF path being considered here. In case a link is bypassed, step 7 should be followed and the VectorSPF contains an emergency path which results from the alternative path, generated in step 3, which continues until it meets a node of the original SPF path. In case a node is bypassed, step 8 should be followed and the VectorSPF contains an emergency path which results from the alternative path generated in step 4, which continues until it meets a node of the original SPF path.

An emergency path that becomes a VectorSPF identifies the extent to which a recovery path must go, since from this intersection point on, the deviated packets may follow normally the same path previously defined by the SPF.

After generating all the VectorsSPF for all the SPF paths destination nodes affected by the simulated failure, they should be fulfilled in the FIB using all the network prefixes announced by each destination node calculated. These data are obtained from the link state information flooded by all the nodes in the topology. This step is not described in the heuristic because it is not part of the emergency path calculation, but of a FIB fulfillment routine.

All the network prefixes announced by the same destination node should refer to a respective VectorSPF only, i.e. that which bypasses the failure and has an emergency path to attain the destination node in question. All the flows aiming those network prefixes should follow this same VectorSPF, reducing the amount of memory necessary in the FIB.

The algorithm proposed here is of a polynomial time and was proved in [23]. Its complexity, in the worst case, is $O(n^3)$, where $n$ is the number of nodes in the topology. It is important to emphasize that the complexity of the IncrementalSPF used in this study is of the worst case, i.e. $O(n^2)$, and one that has as many active interfaces in a node as the number of nodes in the topology (full-meshing).

### 2.5 FEP_proactive Considerations

The heuristic of the proactive part of the FEP schema generates vectors which are available in the FIB to be consulted and used by a reactive approach, or by any proactive signaling approach, which can prompt this path for the moment a failure is detected. The extension of the emergency path is just as long as it takes to allow the deviated flows to follow the SPF original path. The path cost tends to be lower than the one proposed in [6] particularly in terms of resources, since the emergency path extends only to the point that is necessary in order to bypass a failure without causing routing loops.

This heuristic should be executed together with the routing algorithm, then, in case there are any changes in the topology configuration, such as the addition of new nodes or links, the change must pass to the calculation of the VectorsSPF in order to allow for emergency paths updated according to the link state.

In the worst case, the length of an emergency path is as high as the alternative path, which indicates a path which the only intersection point with the original SPF path constitutes the destination node. The possibility of this worst case to happen tends to decrease as the network topology expands. That is because the higher the amount of nodes in an original SPF path the higher the possibility of an intersection between the alternative and the original SPF path to occur before destination node.

Along the transient failures described in [11] and [13], the forwarding information generated by the OSPF and contained in the FIB must be temporarily avoided since they cause instability. In doing so, a reactive approach must stipulate a suppressing/contention time for the OSPF forwarding and for the OSPF reaction to the failure. During this time, make use of the VectorSPF. This reactive approach is still under study by these authors, and it should be publish in future articles. At first stance, the reactive approach suppressing/contention time must be stipulated to run in about 1 minute, observing the results already pointed out in [11] and [13]. During this time, being the failure state detected, the path indicated in the respective VectorSPF should be used. If this path is a shortest path with the same cost as the original shortest path, i.e. ECMP path, or if this path follows the LFA restriction [1], the packet flows should be forwarded, without any modification to establish this path, because it guarantees a path without routing loop. Otherwise, this path must be used through signaling (in order to establish a path), be it a proactive way or a reactive way, because the emergency path will experience routing loop. Once the path is signaled and ready, a reactive approach uses a simple IP packet marking to redirect the packet flows without encapsulating them. This will guarantee a recovery without the existence of routing loops in any situation.

In case the failure exceeds 1 minute, the suppressing time of the OSPF reaction should expire allowing for the announcement of the new link state for every node in the network. Meanwhile, the VectorSPF still continues being used and only stops when the FIB is updated by the OSPF and by the new calculation of the VectorSPF. After the updating, the OSPF forwarding can be normally used.

As all the approaches described in section 1, especially the [6] approach, all the FEP schema [23] must be implemented in all nodes in the OSPF area to offer full single failure repair coverage. For this reason, the use of any VectorSPF, that needs signaling to create a recovery path without routing loop, must exchange information with other nodes in this path.

Like [6], this approach needs some extra state to be stored in each node. The exact value is highly dependent on the way the heuristic is implemented, but at least some memory to store the VectorSPF in FIB will be needed and it depends on how many destination nodes are affected in the topology. We believe that the capability of reusing VectorSPF entries will save some memory use, allowing a scalability factor for this approach. We are working on some tests to estipulate this factor and to reuse some extra state also stored in other nodes – which should be developed in a future work.
It is important to highlight that the QoS requirements can be compromised in the emergency path. This is due to the objective of its calculation which consists in expanding the reliability of a network in general, without adding great complexity to the OSPF. However, seeking paths based on restrictions [3], which obey certain QoS requirements, can become feasible if the parameters to obtain the emergency path are modified, thus, restricting the viable solutions for certain QoS requirements. These paths can be used only by some selected flows with class of services, and the selection being done by a reactive approach. This addition of functionality of restrictive paths implies higher complexity in executing the algorithm [3]. A way to realize such adaptation is still under study by these authors.

Although not taken into consideration in this study, the algorithm support for Shared Risk Link Groups (SRLG) can be viable as long as the OSPF routing algorithm provides support. A SRLG is identified by means of a spot in the physical topology where there are links which share the same area, e.g. optical fibers and equipment which use the same duct. In order to bypass a SRLG, special information need to be exchanged in the link state throughout all the nodes of a topology, indicating which nodes or links belong to a same region SRLG. Some modification in the OSPF message exchange must be done, such as that recently available in [27]. The heuristic can be modified, particularly in step 6, in order to generate VectorsSPF with paths able to bypass these network components, though it needs SRLG information. However, it has not been included in this article since the implementation [27] is not largely spread yet.

Finally, this study does not cover yet multicast traffic reliability, but in a first stance, such reliability could be attained in a similar way to unicast traffic, dealt with in this article. However, further research is needed in order to adapt the FEP_proactive heuristic to generate VectorsSPF for a better multicast reliability.

3. CONCLUSION

This article presented the proactive approach of the FEP schema so called FEP_proactive, which provides a heuristic to generate emergency paths updated with the link state information. These emergency paths are mainly characterized as simple shorter paths which use only the necessary network resources to bypass a failure. The heuristic results in VectorsSPF available in each router FIB. These SPF Vectors offer recovery paths to reach the destination nodes of the packet flows affected by a failure. One fact to be observed is the temporary nature of these recovery paths, i.e. to be used only in fast rerouting during instability periods of transient failures. Once calculated and made available, these paths can have several uses in IP networks. One instance is signaling the path and packets marking, which these authors are still researching. Another future study is aimed at the adaptation of FEP_proactive to more than one OSPF area. Moreover, these paths can even be adopted in MPLS technologies, guiding the establishment of a recover LSP. In making these paths available, independently of the technology, this study looks forward to help an increase of network reliability, and at the same time, a decrease in problems related to transient failures.

4. REFERENCES


