Intra Autonomous System Overlay Dedicated to Communication Resilience

Simon Delamare and Gwendal Le Grand

TELECOM ParisTech (ENST) – LTCI–UMR 5141 CNRS,
46 rue Barrault, 75634 Paris Cedex, France.
delamare@telecom-paristech.fr legrand@telecom-paristech.fr

Abstract. Some services delivered in IP networks, like IP television, Telephony over IP and critical services, have strong robustness requirements. Consequently, the communications delivering those services must be resilient to failures in the network. This paper proposes a new approach to improve communication protection. It consists in deploying a routing overlay dedicated to resilience in an autonomous system, and it reduces connectivity restoration time after a failure (compared to standard routing protocols). Finally, we validate this proposal under different scenarios on an emulated testbed.

Key words: Resilient Networks, Overlay Routing, RON, OSPF

1 Introduction

New services, such as telephony or video on demand have been emerging in IP networks during the last decade. Today, most Internet Service Providers (ISP) propose ”triple–play” subscriptions, consisting in providing telephony and television services in addition to traditional Internet access. These new services create new constraints, particularly in terms of delivery time and bandwidth consumption. Moreover, availability and resilience are strong requirements in the case of television or telephony services. Availability need become even higher when these services are used in a critical framework (e.g. medical communications). It is thus necessary to deploy protection measures to allow reliable service delivery in case of failures or disturbances in the network.

Today, routing protocols are not suited to communications for which resilience is essential, because they do not support fast connectivity recovery after a node or link failure. Indeed, routing algorithms and protocols typically require several tens of seconds to restore connectivity between the nodes [1]. In addition, they do not take into account traffic specificities associated with new services.

In this article, we study a new approach to restore communications in case of failure, which is based on a specific use of an overlay network. Communications are usually organized in layers and are composed of a succession of overlay networks. Our approach consists in deploying an additional overlay dedicated to communication robustness. We separate the two following tasks which are usually ensured by the routing protocols: routing tables advertisement and connectivity recovery in case of a failure. A dedicated system deals with the second task and allows for faster recovery after a failure and thus, improved service delivery to the user. To illustrate this approach, we will deploy an overlay routing protocol inside an Autonomous System (AS), and compare its performance with a network layer routing protocol. The major contribution of this paper is therefore the description of this solution and the study of its behaviour using an emulated network.

The remainder of this document is organised as follows: section 2 describes related works, section 3 presents our approach and discusses its relevance, section 4 discusses the test environment and results. Finally, we conclude and present future works.

2 Related Work

2.1 Dynamic Routing

Dynamic routing protocols automatically compute routing tables in networks. There are two categories of protocols: Internal Gateway Protocols (IGP) and External Gateway Protocols (EGP). EGP are dedicated to routing between different AS and are thus out of the scope of this paper which focuses on intra–AS protection. IGP either use distance vectors (RIP [2], IGRP[3] , EIGRP [4]) or link states (OSPF [5], IS–IS [6]).

The metric used to evaluate the cost of the calculated path is an important parameter which impacts the efficiency of the communications. For example, OSPFs metric is the total bandwidth, which is not adapted to the constraints of a particular traffic because it does not optimise the route for a specific traffic. Extensions of OSPF [7, 8] introduce new metrics such as the delay and the available bandwidth that take into account quality of service requirements.

The robustness of communications directly depends on the frequency of Hello Messages sent by routers to their neighbours, as well as the time (Dead Interval) after which the link is considered to be down if no Hello Message is received. Indeed, the more frequent Hello Messages are and the shorter the Dead Interval is the faster failure detection can be performed. However, too short periods may introduce false positives for which the link is considered as being down whereas it is simply congested [9]. Various solutions were proposed in order to improve link failure detection time while minimizing false positives probability [10, 11].

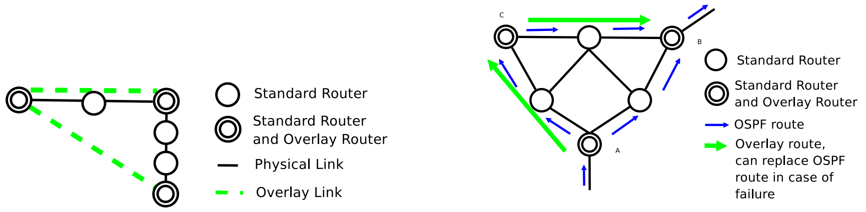
Proactive mechanisms which compute secondary routes used as backups of primary routes [12–15] were proposed to reduce routing protocol recovery time. Other mechanisms are also intended to accelerate route re–computation once a failure is detected [16, 17]. Finally, some mechanisms used with MPLS [18] achieve a good resilience using label switching instead of classical routing.

2.2 Overlay Networks

An overlay network is a logical network built on top of an existing network. A subset of the physical network is selected to take part in the overlay. Overlays are actually present in several systems. For example, the MPLS Virtual Private Network [19] deploy a logical private network on the top of the existing network and Peer To Peer systems [20, 21] create a network between users sharing resources.

Some overlay systems are dedicated to routing [22, 23]; like standard routing protocol, they compute routing tables to establish connectivity between overlay nodes. These systems aimed at solving Border Gateway Protocol (BGP) [24] and inter–AS routing issues. Indeed, routes computed by BGP are not optimal in terms of performance because they are subject to administrative constraints. Moreover, when a failure occurs, several minutes may be needed to restore connectivity [25] because it is necessary for the intra and inter–AS routing protocols to converge.

Contrary to standard routing in which routers are directly connected by physical links and exchange routing information on these links, overlay links completely rely on the mechanism which creates the overlay network. Thus, two disjoint overlay links may share the same physical link and consequently, an identical routing message intended to two different overlay routers can be in fact waste bandwidth inefficiently if they are propagated through the same physical link (cf. Fig. 1(a)). Topology aware protocols take into account the physical network topology to construct the overlay. Their impact on performance was demonstrated in [26, 27].


Standard Router
Standard Router and Overlay Router
Physical Link
Overlay Link
C
B
A
Standard Router
Standard Router and Overlay Router
OSPF route
Overlay route, can replace OSPF route in case of failure

(a) Overlay and physical links

(b) Traffic interception by overlay

Fig. 1. Overlay networks

Resilient Overlay Network [23] (RON) is a routing overlay protocol which may use different metrics to compute routes using a link state algorithm. The architecture of the overlay topology used in RON is Full Mesh, which means that each router is linked with all others routers by an overlay link. Thus, the dissemination of routing messages by RON nodes may use the same physical links within the physical network, especially in small networks in which RON nodes are physically close to each other.

When packets belonging to RON traffic is received by a RON enabled router, it encapsulates and sends the packets to the next hop RON router (based on the RON routing table and the destination IP address) as shown in Fig. 1(b).

The last RON router on the path decapsulates the packet and sends it to its destination.

The quality of a RON route is evaluated by sending periodic probes every 12 seconds plus a random time interval of up to 4 seconds. If a RON node does not obtain any response (from one of its RON neighbours) to a probe within a 3 seconds delay, it sends a series with a reduced interval of 3 seconds. After 4 consecutive probe losses, the link is considered down. This mechanism allows the detection of a failure in 19 seconds on average [23].

3 System Presentation and Relevance

3.1 System Presentation

In this section, we introduce our approach, and explain its relevance. Overlay routing was originally intended to be deployed in the Internet to solve problems caused by routing between various ASs. Therefore, our approach is original because we propose to use overlay routing inside an AS network.

Actually, we use overlay routing in a single AS in order to highlight other benefits of overlay routing. We show that overlay routing provides robustness to critical communications. Indeed, overlay routing allows routing according to the needs of a specific traffic (which is not possible with standard routing protocols). Our approach consists in clearly separating the role of the routing protocol, namely to compute routing tables, and the role of the overlay routing, which is dedicated to protect critical traffic in the network.

Overlay routers are selected among the networks routers so as to provide an alternative route in case of failure on the primary route computed by the routing protocol on the network layer. When such a failure occurs, the overlay router intercepts the traffic and redirects it towards another overlay router in order to circumvent the failure and to improve communications reliability. When several critical communications are present in the network, the various overlay routers dedicated to their protection collaborate in order to share information on network states. This collaboration also makes it possible to limit the number of overlay routers in the network so as to increase the effectiveness of the system in terms of communications re–establishment time. Thus, overlay routers are selected among the routers of the network according to two principles:

- Overlay routers must propose an alternative route in case of failure of any link used by the communications that should be protected
- If an overlay router dedicated to a communication protection can provide another communication an alternate route which satisfies the needs of this communication, it is not necessary to use a new overlay router to protect this new communication.

3.2 Advantages in Using Overlay

One might think that such an overlay system (compared to optimised routing protocols) will not significantly improve communications robustness. However, there are several qualitative advantages in deploying a routing overlay. Firstly, an overlay recovery system is safe and easy because it does not require a modification of the original network. Therefore:

- Router configuration is unchanged. This prevents errors in routers configuration that would disturb the original network.
- The overlay routing system can be deployed without stopping the system thus preserving communication in progress.
- A dysfunction in the overlay system would only affect additional the overlay and its additional functionalities, but not the original system.
- The overlay can be used to deploy new protection mechanisms, like pre–calculated alternative routes, without implementing complex mechanisms in each router.

The other advantage of our solution is its efficiency in terms of robustness. Indeed:

- The overlay has an applicative vision of communications. Using application layer information makes it possible to take routing decisions by considering the entire characteristics of the communication flow, like the type of traffic.
- Using an overlay allows protection of a specific traffic, between given nodes, and thus deploy protection mechanisms in an optimized way (by protecting only critical traffic) without wasting resources by protecting insensitive traffic.

In the following section, we show that overlay routing in an ISP network can improve performance in terms of time of recovery and bandwidth consumption.

4 Proposed Deployment

4.1 Network Architecture

The network architecture used in our approach is shown in Fig. 2. This architecture is a subset of the national network of a French ISP named Free [28]. We selected only a subset of the network in order to preserve the networks part which provides the most connectivity between nodes and proposes alternate routes.

To perform the test, we implement networks routers using Qemu [29], in two computer hosts. In each zone of the figure 2, a computer emulates routers of its zone. Qemu allows a complete computer emulation, with its processor and its network interfaces. A computer emulated with Qemu behaves exactly like a normal computer. It is thus possible to install an operating system and all the desired software without making any modification. In our experiments, we used the FreeBSD 5.4 operating system and the MIT's implementation of RON [30].

Network interfaces are also emulated with Qemu, and all the traffic sent to an emulated interface uses a pseudo interface "tap" of the host machine. In order to ensure connectivity between emulated machines, we connect the "tap"

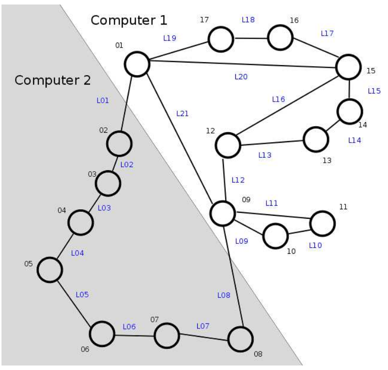


Fig. 2. Test network

emulated interfaces to a network bridge. To ensure connectivity between hosts and thus the two zones of the emulated network, we connect to a network bridge the inter–zone ”tap” emulated interface to the Ethernet network, linking the two computers.

In order to introduce delay into the emulated links, we use Linux Traffic Control [31] applied to pseudo interfaces ”tap”.

The advantages in using such an emulated architecture rather than simulation are manifold since measurements are done in real conditions on wide–area network, while using few physical machines.

4.2 First Scenario

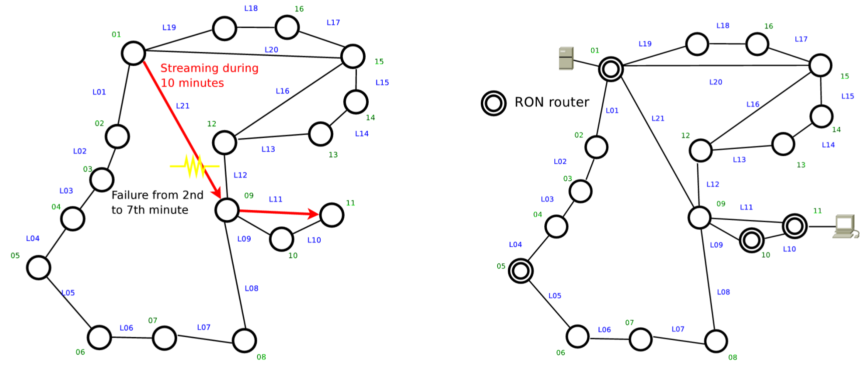
The goal of this scenario is to evaluate the behaviour and the performance of our approach in a simple case and compare our solution with an existing standard routing protocol.

As shown in Fig. 3(a), the scenario consists in streaming a video from computer 01 to computer 11. At 2 minutes of streaming, we cause the failure of the link L21 and carry out its re–establishment 5 minutes later. The video is transported by UDP protocol and has an average bitrate of 1.5 Mbit/s.

In order to compare our approach with existing solutions, we consider the following scenarios:

- OSPF, configured with the default settings.
- OSPF, configured with aggressive probing parameters.
- OSPF with the default settings and RON deployed on nodes 01, 05, 10 and 11 (Fig. 3(b)).

The parameters of the OSPF aggressive probing are chosen in such a way that link failure detection is possible in an average time of 19 seconds (equal to the average time needed by RON to detect link failure). To support this, we set the ”Hello Interval” parameter to 2 seconds and the ”Dead Interval” parameter to



(a) Scenario 1 progress (b) Overlay network

Fig. 3. The first scenario

20 seconds (see Section 2.1). In that configuration our scenarios can be compared in a fair way.

RON is deployed on nodes that can propose alternate routes in case of link failures on the primary route. Therefore, we deployed RON on router 05, to circumvent the failure of the L21 link and on router 10, to circumvent the failure of the L11 link.

Figure 4 shows the forwarding video delay as a function of time, when router 11 receives a video stream. We notice that OSPF does not restore communication at all. Indeed, at the end of the 7th minute, when the link is restored, OSPF has not yet computed new routes to forward the video (in fact, we measured that it would take 362 seconds for OSPF to restore the connectivity between node 01 and node 11). Moreover, from the 500th second until the 560th second, a new route is used by the video stream which circumvents L21 link, even though it has been restored. OSPF actually detects L21 failure, but the link is restored before OSPF computes new routes and updates the routers routing tables. OSPF with aggressive probing needs 200 seconds to restore connectivity (it needs an average time of $200 - 19 = 181$ seconds to update its routes once the failure is detected). RON takes 97 seconds to restore connectivity so it needs 78 seconds to restore connectivity once the failure is detected, which constitutes an improvement of more than 100 seconds with respect to OSPF.

We can explain in detail the various phases of the experiment with RON by studying Fig. 4. Initially, the video is streamed through the shortest route (L21 and L11). When the link is cut, node 11 does not receive the video anymore. But after the 200th second, RON finished new route computation, and the video is forwarded through node 05, then directly to node 11 via node 09. Indeed, from node 05, the video uses the shortest path to go to node 11; it is the OSPFs computed route. Then, around the 500th second, the video uses the L20, L16, L12 and l11 links. OSPF computed a new route to reach node 11 which circumvents L21. RON also re–established the connectivity between node 01 and 11 and

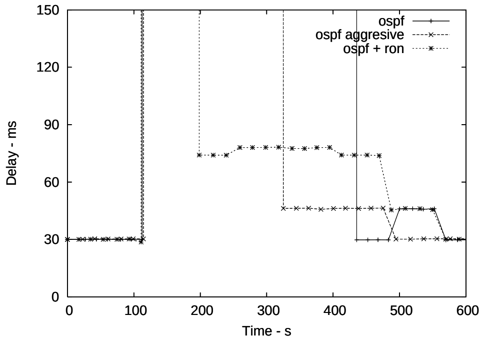


Fig. 4. Delay variation at reception

decided to use this overlay route. At the end of the experiment, OSPF took into account the re–establishment of L21 and updated its routes consequently. So, the video is streamed again through L21 and L11. This operation is transparent for RON which continues to use the overlay link from node 01 to node 11 to forward the video.

We measured the amount of routing messages on L01 druing the entire test. The results are presented in Table 1. We note that the measurement of routing messages during the use of RON also includes OSPFs routing messages. These measurements must be interpreted in a careful way because the number and size of RON messages depend on design and implementation choices, some of which are not relevant in our framework. However, RON does not use an excessive amount of bandwidth in comparison to OSPF configured with similar probing parameters.

Table 1. Volume of messages measured on a link during the entire test

Situation	Volume of messages
OSPF	29.4 kB
OSPF agressive probing	114 kB
RON + OSPF	132 kB

This test has highlighted the effectiveness of overlay routing compared to standard routing to restore a communication in case of failure. Indeed, although RON and OSPF use the same link state algorithms for route computation, RON re–establishes connectivity after a failure in half of the time required by OSPF (with identical average failure detection time). This can be explained by the number of nodes which take part in the routing system is lower in overlay routing than in standard routing. This allows a faster re–establishment of connectivity because computation of routing tables is less complex, the number of participant being less important. Therefore, information on link states takes less time to be propagated to every participants of the overlay than to every router, since the complexity to establish connectivity between each participant increases with the number of participants. Time needed to restore connectivity between nodes is shorter in the overlay routing system, so overlays are more effective than standard routing for communications protection.

4.3 Second Scenario

The second scenario will highlight the different possibilities for overlay deployment. The selection of nodes taking part in the overlay will have an impact on:

- Bandwidth consumption by routing messages. Indeed, the number of control messages exchanged in the network increases with the number of routers.
- New routes computation time, for link state algorithms. Indeed, the algorithm computation complexity depends directly on the number of nodes which take part in this computation.
- The number of alternate routes which can be proposed. Indeed, a significant number of nodes will allow providing more alternate routes and thus, will allow choosing those with optimal routing quality (ie: minimising delay penalty, for example).

It appears that the optimal solution for the overlay routers choice is to minimize the number of nodes while trying to maintain an alternate route satisfying the protected traffic constraints.

Thus, our second scenario consists in streaming the video to four clients, namely nodes 05, 11, 14 and 16. We consider three approaches to deploy the overlay:

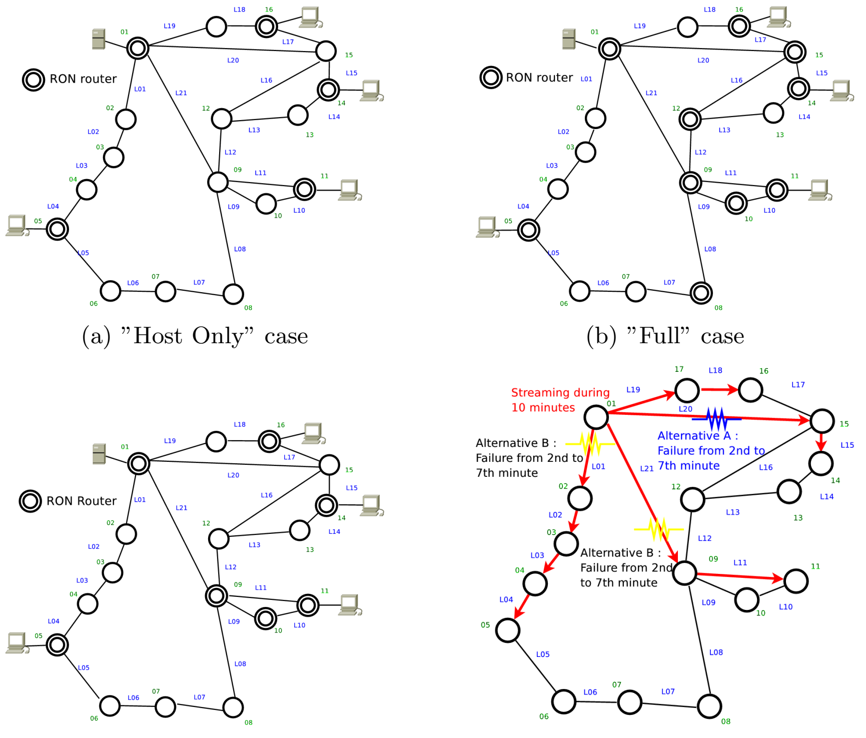
- The overlay nodes are the servers and the clients routers. It is the "host only" deployment of the overlay (Fig. 5(a)).
- The overlay nodes are chosen to protect each communication in an individual way (Fig. 5(b)). For each clients router, we lay out RON nodes to propose an alternate route. This is made independently for each client server communication, and we do not consider already deployed RON nodes to protect another communication.
- The overlay nodes are deployed in an optimized way, i.e. contrary to the previous case, we deploy RON nodes by considering the four client server communications (Fig. 5(c)). Here, we also choose RON nodes so as to propose an alternate route in case of failure of any link on the primary route, for each communication (but node selection is done empirically).

The three approaches correspond to three possible deployments with different goals which constitute the following cases:

- The **"Host Only"** deployment: minimise the number of nodes with the risk of not being able to provide an alternative route in case of failure.

- The **"Full"** deployment: The insurance that for any possible link failure, a route will be proposed, at the cost of deploying many overlay nodes and thus decreasing system performance.
- The **"Optimized"** deployment: A trade–off between the two previous scenarios, in which we wish to provide an alternate route for each possible link failure, while minimising the number of overlay nodes to preserve system performance.

As in the first scenario, video streaming is performed during 10 minutes, but two alternatives are studied. At 2 minutes, we cause the failure of L20, for the A alternative of the scenario. For the B alternative, we cause L21 and L01 failure. At the 7th minute, the links are restored. Figure 5(d) illustrates this scenario.


RON router
RON Router
Streaming during 10 minutes
Alternative A : Failure from 2nd to 7th minute
Alternative B : Failure from 2nd to 7th minute
Alternative B : Failure from 2nd to 7th minute

(a) "Host Only" case

(b) "Full" case

(c) "Optimized" case

(d) Scenario 2 progress

Fig. 5. The second scenario

We measured service interruption time after the failure. The results are presented in Table 2. We note that RON systematically outperforms OSPF (configured with probing parameters equivalent to those of RON). In addition, the time needed to restore connectivity after a failure decreases with the number of nodes taking part in the overlay.

Table 2. Recovery time for different scenarios

Situation	Recovery time		
	To node 14, Scenario 2A	To node 11, Scenario 2B	To node 5, Scenario 2B
OSPF agressive probing	208 s	166 s	387 s
Host Only deployment	127 s	95 s	248 s
Full deployment	142 s	142 s	315 s
Optimized deployment	132 s	128 s	298 s

In order to compare link quality proposed by overlay routers with the various deployments, we measured the forwarding delay penalty generated by re–routing. Delay penalty is a good indicator of routes quality because delay is the metric used for the choice of a route in this test. Table 3 presents the average route delay penalty the communication between node 01 and 11 in alternative B. This penalty is measured between the 300th and 500th seconds, because during this period the traffic is re–routed for all the deployments investigated. In accordance with our expectations, the higher is the overlay router number and the weaker is the over cost of delay (and so, the better is the proposed route quality).

Table 3. Average delay penalty when re–routing between nodes 1 and 11 in the second scenario, alternative B

Situation	Delay Penalty in millisecond
OSPF agressive probing	17.01 ms
RON (”host only” deployment) + OSPF	41.28 ms
RON (”full” deployment) + OSPF	28.73 ms
RON (”optimized” deployment) + OSPF	29.30 ms

To summarize, the ”host only” RON deployment provides best performance for connectivity recovery but with less backup routes and thus less route quality (as shown by the delay penalty measurements). The ”full” RON deployment leads to poor connectivity recovery performance but allows with high route quality. Finally, the ”optimized” RON deployment represents a good compromise. These results confirm the importance of overlay router selection in system efficiency, and their impact on the trade–off between connectivity re–establishment time and backup route quality.

5 Conclusion and Future Work

We discussed the use of overlay routing for the communications protection in a intra–AS network. First, we introduced the requirements for communication protection in today's networks. Then, we presented existing mechanisms which try to provide such protection, and focused in particular on routing overlays like RON (which are easy to deploy and can take into account high level information to make routing decisions) in an intra–AS environment. We showed that this solution improves communication robustness. We also highlighted the importance of the selection of nodes participating in the overlay. We demonstrated that when the number of overlay routers increases, the quality of the routes improves but the connectivity recovery time after a failure increases.

Thus, we showed the relevance to use a communication protection system deployed in an overlay network. However, such a system does not exist since existing systems are not specialized in this field. Our test environment used RON, which is, as far as we now, the only overlay routing system for which an implementation available. However, RON was not designed for this intra–AS use and does not brings new robustness mechanisms, such as pre–computed backup routes. Therefore, it is necessary to design a new overlay routing system dedicated to our needs.

Overlay node placement is also very crucial to allow connectivity recovery after a failure. In our test, we located the overlay nodes empirically. In the future, we will study the feasibility of an algorithm to determine the location of overlay nodes optimally, by deploying a small number of nodes at locations which depend on traffic resilience requirements. We will also have to experiment our system in other scenarios, and compare it with other recovery mechanisms such as those presents in MPLS to draw general conclusion.

Acknowledgements. This work was partly supported by the EU ICT Trust and Security FP6 project DESEREC (CN 26600, www.deserec.eu).

References

1. Basu, A., Riecke, J.: Stability issues in ospf routing. SIGCOMM Comput. Commun. Rev. **31**(4) (2001) 225–236
2. Malkin, G.: Rip version 2. Internet Engineering Task Force. RFC 2453 (1998)
3. Cisco: Interior gateway routing protocol. http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/igrp.htm
4. Cisco: Enhanced igrp. http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/en_igrp.htm
5. Moy, J.: Ospf version 2. Internet Engineering Task Force. RFC 2328 (1998)
6. Oran, D.: Osi is-is intra-domain routing protocol. Internet Engineering Task Force. RFC 1142 (1990)
7. et al., G.A.: Qos routing mechanisms and ospf extensions. Internet Engineering Task Force. RFC 2676 (1999)

8. Kompella, K., Rekhter, Y., Networks, J.: Ospf extensions in support of generalized multi-protocol label switching (gmpls). Internet Engineering Task Force. RFC 4203 (2005)
9. Goyal, M., Ramakrishnan, K., Feng, W.: Achieving faster failure detection in ospf networks. Proc. IEEE International Conference on Communications 2003, vol. 1, pp. 296-300 (2003)
10. Choudhury, G.: Prioritized treatment of specific ospf version 2 packets and congestion avoidance. Internet Engineering Task Force. RFC4222 (2005)
11. Gao, D., Zhou, Z., Zhang, H.: A novel algorithm for fast detection of network failure. Photonic Network Communications, Volume 9, Issue 1, Pages 113 - 120 (2005)
12. Molnr, M., Tezeghdanti, M.: Reroutage dans ospf avec des chemins de secours. Projet ARMOR, Rapport de recherche n. 4340 (2001)
13. Stamatelakis, D., Grover, W.: Ip layer restoration and network planning based on virtual protection cycles. IEEE Journal on Selected Areas in Communications (JSAC) 18(10) (2000)
14. Medard, M., Finn, S., Barry, R., Gallager, R.: Redundant trees for preplanned recovery in arbitrary vertex-redundant or edge-redundant graphs. IEEE/ACM Transactions on Networking, 7(5):641–652 (1999)
15. Kvalbein, A., Hansen, A., Cicic, T., Gjessing, S., Lysne, O.: Fast recovery from link failures using resilient routing layers. Computers and Communications, 2005. ISCC 2005. Proceedings. 10th IEEE Symposium on , vol. 27-30, no.pp. 554- 560 (2005)
16. Narvaez, P., Siu, K., Tzeng, H.: New dynamic spt algorithm based on a ball-and-string model. In INFOCOM, pages 973–981 (1999)
17. Liu, Y., Reddy, A.: A fast rerouting scheme for ospf/isis networks. http://www.ece.tamu.edu/~reddy/papers/yong_icccn04.pdf
18. Pasqualini, S., Iselt, A., Kirstadter, A., Frot, A.: Mpls protection switching vs. ospf rerouting. Fifth International Workshop on Quality of future Internet Services (QofIS'04), Barcelona, Spain, September 29-30 (2004)
19. Rosen, E., Rekhter, Y., Systems, C.: Bgp/mpls vpns. Internet Engineering Task Force. RFC 2547 (1999)
20. Cohen, B.: Incentives to build robustness in bittorrent. http://bitconjurer.org/BitTorrent/bittorrentecon.pdf (2003)
21. et al, M.C.: Splitstream: High-bandwidth multicast in cooperative environments. Proc. of the 19th ACM Symposium on Operating Systems Principles (SOSP 2003) (2003)
22. et al, S.S.: Detour: informed internet routing and transport. IEEE Micro, Vol.19, Iss.1, Jan/Feb 1999, pp. 50-59 (1999)
23. Andersen, D., Balakrishnan, H., Kaashoek, M.F., Morris, R.: Resilient overlay networks. Proc. 18th ACM SOSP, Banff, Canada (2001)
24. Rekhter, Y., Center, T.W.R., Corp., I., Li, T.: A border gateway protocol 4 (bgp-4). Internet Engineering Task Force. RFC 1771 (1995)
25. Paxson, V.: End-to-end routing behavior in the internet. In Proc. ACM SIGCOMM (Cannes, France, Sept. 1997), pp. 139152. (1997)
26. Li, Z., Mohapaira, P.: The impact of topology on overlay routing service. INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, Vol.1, Iss., 7-11 March 2004 Pages:- 418 (2004)
27. Tang, C., McKinley, P.: On the cost-quality tradeoff in topology-aware overlay path probing. Network Protocols, 2003. Proceedings. 11th IEEE International Conference (2003)

28. Free: Internet service provider. http://www.free.fr
29. Bellard, F.: Qemu open source processor emulator. http://fabrice.bellard.free.fr/qemu/
30. MIT: Resilient overlay network source code. http://nms.lcs.mit.edu/~dga/ron-dist.tar.gz
31. Stanic, M.: Linux qos control tool. http://www.rns-nis.co.yu/~mps/linux-tc.html