A CTMC-based characterisation of the propagation of errors in GMPLS Optical Rings

Isaac Seoane [1], José Alberto Hernández [1], Ricardo Romeral [1], Manuel Urueña [1],
Eusebi Calle [2], Marc Manzano [2], Juan Segovia [2], Pere Vilà [2]

[1] Universidad Carlos III de Madrid
Avda. de la Universidad 30,
E-28911 Leganés (Madrid) Spain
{iseoane, jahgutie, rromeral, muruenya}@it.uc3m.es
[2] Institute of Informatics and Applications (IIiA)
University of Girona
Girona 17071, Spain
{eusebi, mmanzano, jsegovia,pvila}@eia.udg.edu

Abstract

This article presents a Continuous-Time Markov Chain model to characterise the propagation of failures in optical GMPLS rings. In order to characterize the behaviour of failure propagation epidemic-based models are commonly used. However, the existing epidemic models do not take into account the specific features of a multilayer network environment. A node failure in GMPLS-based networks can affect: Control Plane and Data plane reporting different failures scenarios. Consequently, an extended generic epidemic model called SID is proposed, in order to cover multiple failures and recovered states in a GMPLS Multilayer scenario. The CTMC model takes into account the SID model and provides a set of design rules to specify the values of repair rates required to achieve a given service availability, assuming a certain infection and disable rate.

Keywords

Optical GMPLS Rings; Epidemic propagation of errors; Continuous Markov Chains; Reliability analysis.

1. INTRODUCTION AND RELATED WORK

Network reliability and failure resilience has become a major concern for Internet Service Providers and Operators. Indeed, network operators often seek ways to provide the so-called five-nine-reliability level, that is, devising the mechanisms to guarantee that their networks are 99.999% of the time fully operational [1]. Most models consider that network failures occur independently from one another, for instance a fibre cut or node malfunctioning, as isolated events and never related. However, there is a gap in the literature when considering environments at which network malfunctioning propagates across a given topology network. This is typical from virus/worms attacks or due to natural disasters.

In such case, epidemic models can be used to characterise the dynamics of failures that spread from a single node to the rest of the network. The concept of Epidemic Networks (EN) is a general term that describes how an epidemic evolves on a set of individuals during a certain amount of time. The rise and decline of an epidemic may be probabilistically characterised, and definitely depends upon the infection propagation rate and node connection degree [2]. Research in this area involves the study of different aspects, including how the epidemic evolves over time or how to immunise part of the population in order to minimise and control the epidemic propagation and effects. Examples of networking applications where EN models may apply include power supply networks, social networks, neural networks or computer networks.

The research community has proposed a large number of epidemic models, mainly focused on characterising the propagation of viruses in biological systems. There are several families described in the literature dealing with models of virus propagation [3]. The first family, called the Susceptible-Infected (SI) considers individuals as being either susceptible (S) or infected (I). This family assumes that the infected individuals will remain infected forever and, so, it can be used as a "worst case propagation" scenario. A less-pessimistic family is the Susceptible-Infected-Susceptible (SIS) group, which considers that a susceptible individual that became infected on contact with another infected one may then recover with some likelihood. Therefore, individuals may change their state from susceptible to infected, and vice versa, several times. The third family is the Susceptible-Infected-Removed (SIR), which extends the SI model to take into account the removed state. In the SIR group, an individual can be infected just once because, when the infected individual recovers, it becomes immune and will no longer pass the infection onto others. Finally there are two families that extend the SIR family: SIDR (Susceptible Infected Detected Removed) and SIRS (Susceptible Infected Removed Susceptible). The first one adds a Detected (D) state, and is used to study the virus throttling, that is, an automatic mechanism for slowing down the spread of diseases. The second one considers that, after an individual becomes removed, it remains in that state for a specific period of time, and then goes back to the susceptible state.

In the case of optical GMPLS-based transport networks, failures may occur in either the control and/or data planes, or in both of them. The former characterises the case at which control functionality becomes unavailable, and the later refers to malfunctioning that also affects packet-forwarding services. Previous work by the authors [4] introduced a new epidemic model called SID (Susceptible, Infected, and Disabled) where a given node may be in any of the following three states: The Susceptible state (both control and data plane are fully functional), the Infected state (when the control plane becomes infected, and may infect other neighbouring nodes) and the Disabled state (if both control and data planes are down). This article formulates the failure propagation across a GMPLS ring as a Continuous-Time Markov Chain (CTMC), and sets the formulation grounds towards its performance characterisation.

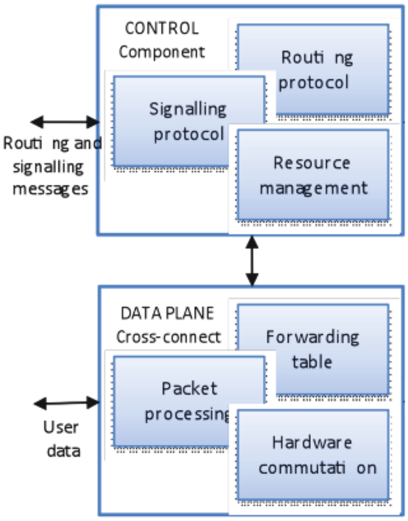

Fig. 1A. GMPLS router architecture: The Control and Data planes

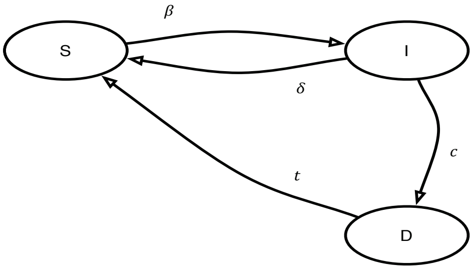

Fig. 1B. State-transition diagram for the SID model

The remainder of this work is thus organised as follows: In section 2, GMPLS-based network failures are explained. Section 3, introduces the SID model. Section 4 presents the error propagation model and its formulation using CTMC concepts. Then, section 5 depicts some numerical results as an example applied on a four-node ring. Finally, Section 6 concludes this work reviewing its main contributions and findings.

2. FAILURES IN GMPLS NETWORKS

Usually, when GMPLS networks are considered (i.e. optical networks), it is possible to distinguish two different parts in every node. On one hand, there is a control plane that runs the control and management software such as routing protocols, signaling protocols, etc. On the other hand, there is a data plane that is dedicated mainly to forwarding user data. In other words, control plane messages and data plane packets could even be isolated (not sharing the same transmission medium) and even have a different topology [5]. In such scenarios (see Fig. 1A) it is possible that some attack or failure could occur that affects only the control plane. If this is the case, then the routing and signalling procedures do not work appropriately, meaning that it is not possible to establish new connections. However, it is possible that the existing configuration before the failure in the data plane could be maintained and current established connections are not dropped, i.e. the data plane continues working properly.

If a virus attacks one node or there is a bad software configuration, it can happen that only a specific function in the control plain fails. For instance, if the signalling module fails but the routing module is still working, new connections cannot be established through that node, and existing connections cannot be removed. In that case, if a fast recovery is not possible, the routing module can be used for advertising “no free capacity available”, in order to avoid having new connection attempts through the failed node. On the contrary, if the routing module fails and the signalling module is still working, the node is still able to process new connection requests and tear down existing connections. In this case, changes in the local state (e.g. capacity being allocated/released) will not be advertised until the routing process is recovered, so other nodes will be working with out-of-date information. In this paper it is assumed that a control plane failure always involves both signalling and routing modules, so as to reduce the number of failure scenarios.

In order to recover the functionality of a failed control plane without disruption of the ongoing connections in the data plane, it is necessary to recover the control plane as soon as possible and re-synchronize the control plane state with the data plane state. This is not easy to accomplish and may take some time due to a first stage of reinstalling or rebooting the control plane and the necessary procedures and protocol messages for that re-synchronization [6]. It is also necessary that nodes implement re-synchronization mechanisms like Non Stop Forwarding (NSF) and Graceful Restart (GR). It could also happen that, some time after the control plane failure, the data plane also fails causing a complete node failure and a disruption of the established connections through that node.

3. ON THE PROPAGATION OF ERRORS IN GMPLS OPTICAL RINGS

This section explains how errors propagate along a GMPLS network following the SID model and the notation to describe it. Only node failures are considered (link errors are not possible in this model). Figure 1A shows the generic architecture of a GMPLS switch.

Under the assumptions of the SID model, every node in the ring may be in either one of the following states:

- The “S” state, which stands for "susceptible state". In this state, both the control planes and the forwarding planes of the GMPLS node operate properly, hence the node is susceptible of becoming infected if one of its neighbours is already infected. Additionally, the node may fail spontaneously, which means that the node is originating a new infection.
- The “I” state stands for “infected state”. In this case, the control plane of this GMPLS-based node fails. In that case, this node is not able to create new LSPs nor it may modify the current configuration of its LSPs. However, the node may still forward traffic from its current configuration since its forwarding plane is still operational. When the node is in the I state, it may propagate errors to its neighbours.
- The “D” state, which stands for “disabled state”. In this case, both the control and forwarding planes are not operational. We consider that a disabled node may still propagate errors to adjacent nodes.

Table I. Summary of failure and repair rates

Parameter	Description
β_F	Spontaneous infection rate
β	Infection propagation rate
c	Disabling rate
δ	Control plane repairing rate
t	Repairing rate of disabled nodes

Figure 1B shows the state-transition diagram for the SID model (Susceptible, Infected and Disabled), where a given node may be in any of the three previous states. The values near the arrows refer to the transition rates between states on a node.

Essentially, Figure 1B states that a node susceptible to be infected (a node that is working properly, i.e. on state S) becomes infected at rate β (if there exists at least one node already infected). An infected node may become again operational (S state) or disabled (D state). The first case occurs at rate δ, which is the rate at which the network administrator fixes the problem, whereas the second case occurs at rate c. The network operator may also repair disabled nodes at rate t. Finally, βF refers to the spontaneous failure rate at which a given node in the network, whose neighbours are not infected, may actually become infected (spontaneously). Table I summarises all model parameters.

4. MODELLING A GMPLS RING: EXAMPLE WITH FOUR NODES

Figure 2 shows a four-node GMPLS ring network. To build the CTMC model, it is important to remark that failure propagation occurs only between adjacent nodes.

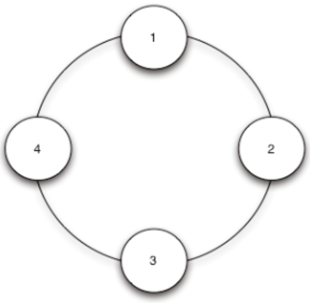

Fig. 2. The four-node GMPLS-based ring example

In light of this, Figure 3 shows the complete state transition-rate diagram of a CTMC model for this particular case of a four-node ring. Each state is labelled with the triple (NS:NI:ND), where NS refers to the number of nodes in the S state, NI denotes the number of nodes in state I, and ND gives the number of nodes in the S state. In this example of ring topology, the states identification labels could take values from the set 0≤{NS,NI,ND}≤4, while satisfying the constraint: NS+NI+ND=4 for every state.

Clearly, the CTMC starts on state (4:0:0), which means that the four nodes are fully operational and no nodes are infected or disabled. The first transition to state (3:1:0) occurs with rate 4βF and takes into account the fact that any of the four nodes become infected spontaneously. The rate is 4βF to take into account the fact that this occurs at four times the rate of a single failure, since we have four nodes susceptible of failure. This is the minimum of four exponentially distributed random variables with rate βF.

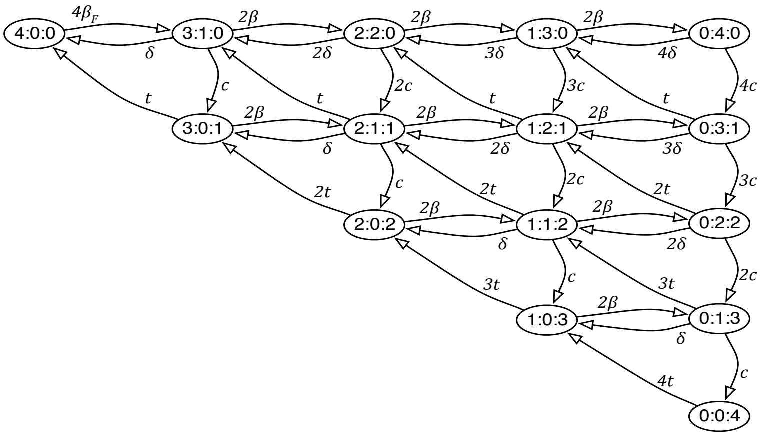

Fig. 3. State transition-rate diagram for a four-node GMPLS ring

Table II. Infinitesimal generation matrix for a 4-nodes ring (Q4)

Q_4	4:0:0	3:1:0	3:0:1	2:2:0	2:1:1	2:0:2	1:3:0	1:2:1	1:1:2	1:0:3	0:4:0	0:3:1	0:2:2	0:1:3	0:0:4
4:0:0		$4\beta_F$													
3:1:0	δ		c	2β											
3:0:1	T				2β										
2:2:0		2δ			2c		2β								
2:1:1		t	δ			c		2β							
2:0:2			2t						2β						
1:3:0				2δ				3c			2β				
1:2:1				t	2δ				2c			2β			
1:1:2					2t	δ				c			2β		
1:0:3						3t								2β	
0:4:0							2δ					4c			
0:3:1							t	2δ					3c		
0:2:2								2t	2δ					2c	
0:1:3									3t	δ					c
0:0:4										4t					

On state (3:1:0), the CTMC may jump to three possible states: firstly, it may jump back to state (4:0:0) if the infected node is repaired (this occurs with rate δ); secondly, the Chain may jump to state (3:0:1) if the infected node becomes disabled (this occurs with rate c); and thirdly, the Chain may jump to state (2:2:0) if the infected node propagates its control plane misbehaviour to one of its neighbour (this occurs with rate 2β because it has two neighbours). It is worth remarking that β>>βF, hence once a given node is infected, the probability to have spontaneous infections is very small compared to infection propagation.

In summary, the CTMC is characterised by the 15-state transition-rate diagram of Figure 3. Additionally, Table II summarises the transition matrix for the four-node ring, which can be used to generate the infinitesimal generator matrix for this CTMC, namely Q4. The empty gaps are assumed zero and the diagonal must equal minus the sum of rates along its row.

With Q4, the steady-state solution for this CTMC requires solving Pi from the following set of equations:

$$P_i q_i = \sum_{j \in C} q_{ij} P_j \qquad for\ i \in C \quad (1)$$

$$\text{where } \sum_{j \in C} P_j = 1 \ \ (2), \text{ and } \quad q_i = \sum_{j \in C} q_{ij} \quad (3)$$

Here, Pi denotes the steady-state probability of state i, C refers to the state space and qij is the transition rate from state i to state j given by the infinitesimal generator matrix QN. The values of Pi give the amount of time that, in the long run, the CTMC stays on every state. It is also interesting to study the probability of certain sets of states, basically, sets of states with a given number of nodes on states S, I or D, as desired. For instance, the probability to have exactly NS* nodes susceptible of infection is:

$$P(N_S = N_S^*) = \sum_{j \in \{C \backslash N_S = N_S^*\}} P_j \quad (4)$$

which just comprises the sum of steady-state probabilities of states (NS*:*:*).From Figure 3, it is easy to observe that this value is the sum of probabilities over the NS*-th column, and we shall refer to this column as . For example, denotes the probability to find the network with exactly three susceptible nodes regardless of the existing number of infected and disabled nodes. In light of this, it is also easy to compute the steady-state probability to find the network with a certain number of infected (NI) or disabled (ND) nodes, again after summing some probability values:

$$P(N_I = N_I^*) = P_{diag\left(N_S N_I^* N_D\right)} = \sum_{j \in \{C \backslash N_I = N_I^*\}} P_j \quad (5)$$

$$P(N_D = N_D^*) = P_{row\left(N_S N_I N_D^*\right)} = \sum_{j \in \{C \backslash N_D = N_D^*\}} P_j \quad (6)$$

This just requires summing the steady-state probabilities of a given diagonal or row in the state-transition rate diagram of Figure 3.

5. NUMERICAL EXAMPLE

Table III shows an example of transition rates following reference [7].

Table III. Model parameters chosen in normalized units (occurrences/time units)

Rate s	4-nodes	100-nodes
β_F	0.01	0.0085
β	0.1	0.085
c	0.1	0.1
δ	0.07	0.05
t	5	5

After solving the steady-state probabilities of the CTMC-based model, it is easy to show the percentage of time that the ring stays in every state as a function of the two repairing rates: the rate δ at which the control plane of a node is repaired (this is, transition rate from the Infected state to the Susceptible state of a node) and the rate t at which nodes are fully repaired (transition rate from the Disabled state to the Susceptible state).

We have summarised the results in Figures 4, 5 and 6, where different Pcol, Pdiag and Prow are shown. In the first plot of Figure 4, we show the steady-state probability of having each possible number of nodes in the up (i.e., susceptible) state for different values of δ and t. Clearly, node failure becomes less likely the larger the value of δ (for a given value of t). As shown, for δ=0.15, the value oft which makes Pcol (4:I:D) approximate unity is t>0.1. However, when δ=1.5, the disabled node repairing rate must be t>0.01. The conclusion from this experiment is that, when the infected repair rate δ is small, the repair rate of disabled nodes must be greater to compensate this. On the other hand, when δ is large, the value of t does not necessarily have to be that large to achieve Pcol (4:I:D) approximate unity.

Figure 5 and 6 show a similar set of results for Pdiag and Prow respectively. It should be pointed out that Pdiag refers to the cumulated probability to find the ring with a given number of infected nodes and Prow gives the cumulated probability to find a given number of disabled nodes.

Figure 5 shows that for δ>0.15, the probability to find Infected nodes is very small (regardless of the value of t). Figure 6 shows that it is required to have t>0.1 to have no disabled nodes with large probability (close to unity) regardless of δ.

In conclusion, for the failure rate parameters of Table II, a value of δ>0.15 and of t>0.1 is sufficient to have all nodes in the susceptible state with large probability (close to unity). When δ<0.15, the values of Pdiag show that more infected nodes are likely to occur. On the other hand, as expected, when t<0.1, then it is the number of disabled nodes which becomes more likely to occur.

Plots are also helpful to determine the values of δ and t required to achieve a certain node availability level, for a given set of infection and disable rates β and c.

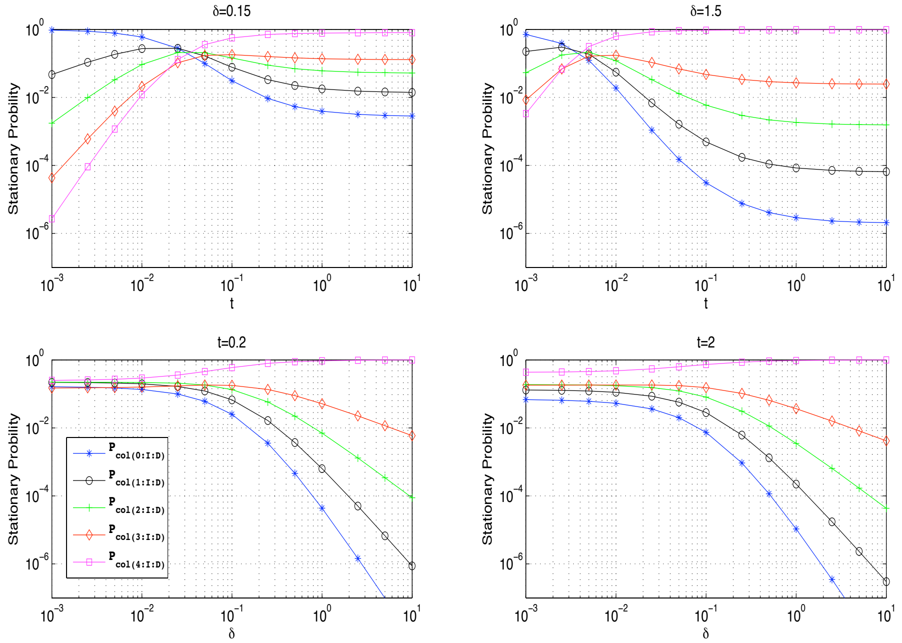

Fig. 4. Steady-state Probabilities for the same number of susceptible nodes (Pcol) existing in the network for different values of δ and t.

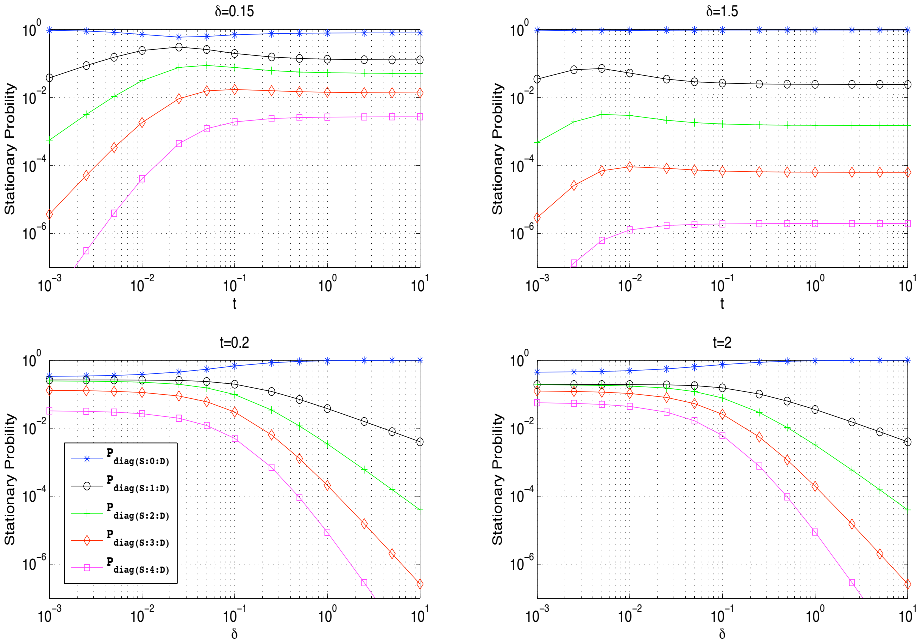

Fig. 5. Stationary Probabilities for the same number of infected nodes (Pdiag) existing in the network for different values of δ and t.

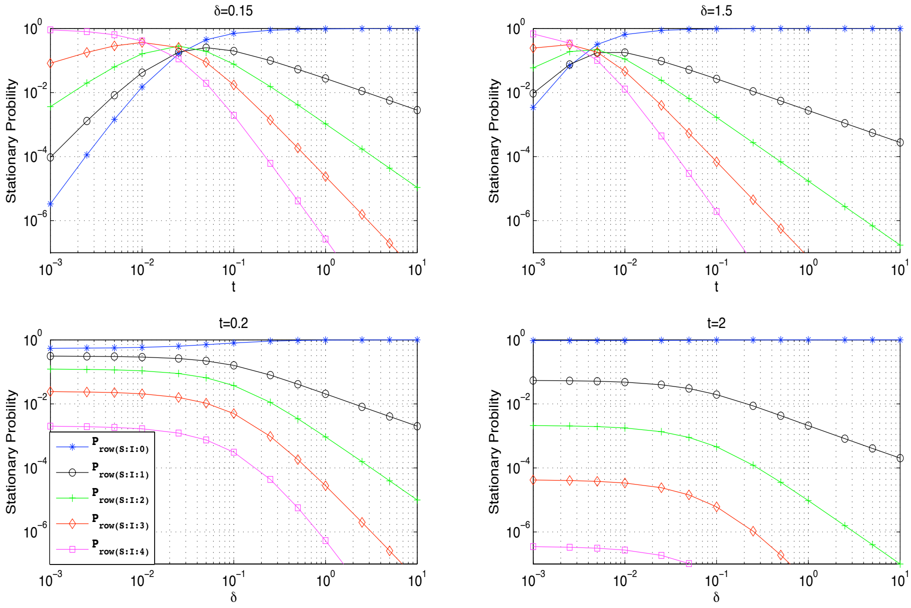

Fig. 6. Stationary Probabilities for the same number of disabled nodes (Prow) existing in the network for different values ofδ and t.

6. CONCLUSIONS

This work has presented a CTMC model to characterise the transient behaviour and possible states of a GMPLS-based network with ring topology whose nodes may become infected or disabled following the SID failure propagation model. A full numerical example has been presented, analyzing the resulting steady-state probabilities for a selected number of δ and t on a four-node ring.

The presented CTMC model can help network operators in finding the required service repair rates of control and data planes to attain a certain level of availability. Additionally, it can be use for studying the sensitivity of the network to different combinations of failure and repair rates, in terms of the expected number of nodes in each state (susceptible, infected or disabled).

ACKNOWLEDGEMENTS

The work described in this paper was carried out with the support of the BONE project ("Building the Future Optical Network in Europe"), a Network of Excellence funded by the European Commission through the 7th ICT-Framework Programme.

Additionally, the authors would like to thank the support of the T2C2 Spanish project (under code TIN2008-06739-C04-01) and the Madrid Community through the MEDIANET project (S-2009/TIC-1468) to the development of this work.

This work is partially supported by Spanish Ministry of Science and Innovation project TEC 2009-10724 and by Generalitat de Catalunya research support program (SGR-1202).

REFERENCES

[1] J.-P. Vasseur, M. Pickavet, and P. Demeester, "Network recovery: Protection and Restoration of Optical, SONET-SDH, IP and MPLS," Morgan Kaufmann, 2004.

[2] M. Barthelemy, A. Barrat, R. Pastor-Satorras, A. Vespignani. "Dynamical patterns of epidemic outbreaks in complex heterogeneous networks," J. Theoretical Biology 235: 275–288.

[3] T. G. Lewis, "Network Science: Theory and Applications". WileyPublishing, 2009.

[4] M. Manzano, J. Segovia, E. Calle, P. Vilà, J. L. Marzo, "Modelling spreading of failures in GMPLS-based Networks,"in Proc. Intl. Symposium on Performance Evaluation of Computer and Telecommunication Systems, July 2010 (Accepted paper).

[5] A. Jajszczyk and P. Rozycki, "Recovery of the control plane after failures in ASON/GMPLS networks," Network, IEEE, vol. 20, no. 1, pp. 4 –10, jan.-feb. 2006.

[6] G. Li, J. Yates, D. Wang, and C. Kalmanek, "Control plane design for reliable optical networks," Communications Magazine, IEEE, vol. 40, no. 2, pp. 90 –96, feb 2002.

[7] P.M. Santiago del Río and J.A. Hernández and J. Aracil and J.E. López de Vergara and J. Domzal and R. Wójcik and P. Cholda and K. Wajda and J.P. Fernández Palacios and Ó. González de Dios and R. Duque "A reliability analysis of Double-Ring topologies with Dual Attachment using p-cycles for optical metro networks". Computer Networks 2009. In Press, Corrected Proof. Issn: 1389-1286.