Failure propagation in GMPLS optical rings: CTMC model and performance analysis

I. Seoane [a,*], E. Calle [b], J.A. Hernández [a], J. Segovia [b], R. Romeral [a], P. Vilà [b], M. Urueña [a], M. Manzano [b]

[a] *Universidad Carlos III de Madrid, Spain* [b] *Universidad de Girona, Spain*

Abstract: Network reliability and resilience has become a key design parameter for network operators and Internet service providers. These often seek ways to have their networks fully operational for at least 99.999% of the time, regardless of the number and type of failures that may occur in their networks.

This article presents a continuous-time Markov chain model to characterise the prop-agation of failures in optical GMPLS rings. Two types of failures are considered depend-ing on whether they affect only the control plane, or both the control and data planes of the node. Additionally, it is assumed that control failures propagate along the ring infect-ing neighbouring nodes, as stated by the Susceptible-Infected-Disabled (SID) propagation model taken from epidemic-based propagation models. A few numerical examples are per-formed to demonstrate that the CTMC model provides a set of guidelines for selecting the appropriate repair rates in order to attain specific availability requirements, both in the control plane and the data plane.

Keywords: Optical GMPLS, rings, Epidemic propagation of errors, Continuous-time Markov chains, Reliability analysis

1. Introduction

Network reliability and failure resilience has become a major concern for Internet service providers and network operators. Indeed, network operators often seek ways to provide the so-called five-nine reliability level, meaning that the objective is to have a fully operational network for at least 99.999% of the time. There are several methods and techniques for dealing with failures so that service continuity is either not compromised in the first place, or it is quickly restored [1,2].

Current networks integrate multiple transport technologies so that the whole system follows a stacked multilayer architecture, whereby the upper layers operate on virtual topologies built successively upon structures produced in the lower layers [3]. Generalised Multi-Protocol Label Switching (GMPLS) is gaining wide acceptance as the protocol suite of choice for managing such heterogeneous networks [4].

GMPLS facilitates the interoperation and convergence of disparate transport technologies through a unified control plane, and aims at easing challenging aspects such as service provisioning, traffic engineering and failure recovery [5]. Despite the fact that a multilayered architecture can improve network resilience as it brings flexibility to fault management and recovery [6,7], it introduces an undesirable effect known as *failure propagation*, whereby failures at the bottom layer may disrupt services in higher layers. Besides this, due to the nature of the multilayer architecture, one failure at the bottom layer can manifest itself as several concurrent failures in higher layers.

The majority of the approaches to network recovery assume that the number of failures whose repair is pending at any given time is small (e.g., one or two), and that they occur independently from one another. The treatment of this type of failure is extensive in the literature, and

* Corresponding author. Tel.: +34 916248794.
E-mail addresses: iseoane@it.uc3m.es, isaacsp@gmail.com (I. Seoane).

all aspects of network design and operation are well covered. However, not such extensive research has been conducted on scenarios of arbitrary large-scale and/or multiple failures. Such failures are usually caused by natural disasters or intentional attacks, and thus are much rarer than, say, cable cuts or malfunctioning of hardware modules, but their consequences are often much severer. This paper aims at furthering our understanding of the impact on the availability of a GMPLS-based network subject to a specific form of multiple failures, namely, the one that spreads from one node to its neighbours through the control plane, possibly affecting a considerable part of the network topology.

A key feature of GMPLS is the separation of the control plane from the data plane, to the point that they can even be deployed on separate networks. Due to this separation, failures may occur in either of the two planes, or in both simultaneously [8]. A failure in the control plane leads to the loss of control functionality (e.g., a switch/node becomes unmanageable), while a data plane failure affects packet-forwarding services [9]. In multilayer architectures, this separation of planes not only brings many benefits, but also a new requirement: the need for resilience in the control plane [8,10]. However, to the best of our knowledge, no study has been published for a scenario in which a control plane failure on a node ultimately provokes a failure in the data plane, that is, a situation in where an inter-GMPLS plane failure propagation exists.

The objective of this paper is therefore to characterise the transient behaviour and possible states of a GMPLS-based optical ring subject to a multiple failure scenario, where the propagation of failures occurs simultaneously on two axis: horizontally in the control plane, from node to node, and vertically from the control plane towards the data plane. A continuous-time Markov chain model is used for assessing the reliability of such ring topology.

The remainder of this work is organised as follows: In Section 2, GMPLS-based network failures are explained. Section 3, introduces the Susceptible-Infected-Disabled (SID) model, which is the basis of the error propagation model introduced in Section 4. Then, Section 5 depicts some numerical results as an example applied on a eight-node ring. Finally, Section 6 concludes this work reviewing its main contributions and findings.

2. Related work and problem statement

2.1. Failure propagation in multilayer networks

The negative effects of failure propagation can be avoided or limited by having the network's lower layers automatically finding or using new paths or subpaths after a failure, provided they have their own protection mechanisms. Thus, recovery procedures can be automatically activated upon failure transparently to the upper layer [11].

A different approach is to design the higher-level network topology taking into account the capabilities and constraints of the network's lower layers. Thus, when designing IP over WDM networks, traffic demands from the IP layer are allocated over the WDM infrastructure such that, in case of node failure or fibre cut, (a) the IP topology is still connected, and (b) there is enough capacity to successfully complete the recovery at the IP layer. This problem is often referred to as network mapping (or survivable mapping) and is known to be NP-complete [11]. Several heuristic algorithms have been proposed in the literature to find such mappings, or to augment the topologies until the appropriate mapping is found, see for instance some related works: [12–14], or the more general studies: [15,3,16–19].

Most of the research in survivable optical networks, including those concerned with multilayer networks, assume that failures occur independently from one another. Thus, instances of failures such as fibre cuts and node malfunctioning are usually modelled as isolated and unrelated events. Furthermore, as multiple failures are considered possible but rare [20], the focus tends to be on single failures, and on single link failures in particular, with only a few studies tackling the design of networks capable of withstanding up to double link failures. Nonetheless, one specific form of multiple link failure that attracted much attention is that resulting from damages to physical structures, such as ducts, that are shared by otherwise unrelated fibre links. The concept of "Shared Risk Link Groups" [21,22] and its generalisation "Shared Risk Resource Groups" (SRRG) [23], capture this situation and have been used extensively in network survivability design. However, this study addresses the case of failure propagation across nodes in a networks, which is a very different topic to the classical network reliability analysis with isolated (and uncorrelated) failures.

Many more disrupting failures, however, can be found in the real world. These include the ones in which the malfunctioning can propagate through the network, or cover a large geographical area, thus affecting several completely unrelated network elements simultaneously. Root causes of such large-scale failures are typically natural disasters [24,25], but can also be virus/worms outbreaks as well as intentional attacks [26]. Although the literature on large-scale failures is vast in the context of the study of complex networks (see for example [27–29] and the references therein), far less research is published on the modelling or the analysis of such failures in data networks. Some well-published catastrophic failures are analysed in [30,31] but they are not directly applicable to transport networks, as they address the impact on the IP layer of the global Internet.

Geographically correlated network failures affecting specific locations are studied in [32,33]. They provide models to evaluate reliability on given failure scenarios so as to determine the most vulnerable areas of the physical network. The focus is on the structural properties of given topologies and their ability to withstand localised disasters caused by non-propagating failures.

2.2. Failures in GMPLS-based networks

Usually, when GMPLS networks are considered (i.e. optical networks), it is possible to distinguish two different parts in every node (see Fig. 1). First of all there is a forwarding component where specifically designed hardware is dedicated to processing, as quickly as possible, incoming

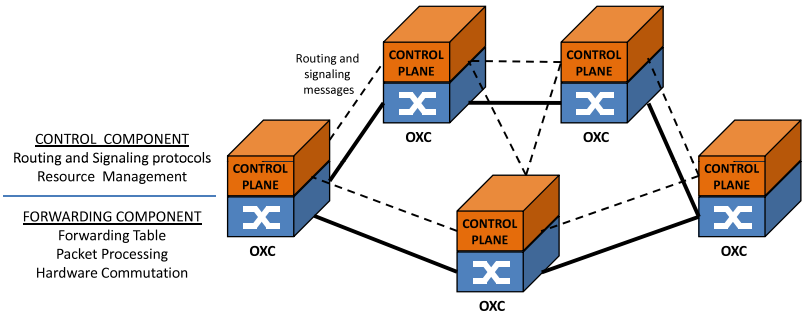


Fig. 1. The control and data planes in the GMPLS architecture.

data packets to their corresponding output ports in accordance with a forwarding table. Above this component there is a generic control hardware executing a specific network operating system that runs the routing and signalling protocols and configures the forwarding table (when connections are established or released). Although both components are usually located in the same device, they have some degree of isolation from one another. They can even be placed in different devices and have the control messages sent through a different network [8].

In such scenarios it would be possible for an attack or failure to only affect the control component or only the forwarding component, for a short or mid span. It is even possible that, due to a virus, targeted attack or software configuration error, the failure only affects to a single control plane mechanism (i.e. signalling protocol or routing protocol). In the case that the signalling module fails and the routing module is still working, connections cannot be established or removed through that node. In this case it is possible to use the routing module to advise the neighbours that there is no free capacity available so they do not attempt to establish new connections through the partially failed node. On the other hand, if the signalling module is still operational but the routing module fails, changes in the local state (e.g. capacity being allocated/released) will not be advertised to the neighbours and they will be working with out-of-date information. However, the failed node could still be able to process new connection requests and tear down existing connections.

In this work we assume that a control plane failure involves both signalling and routing failures. In this case, it is not possible to establish/release connections, and neighbours will work with out-of-date information whenever a control failure occurs. However, it is possible that, for some time, the forwarding component continues working properly with the forwarding table configured appropriately for the connections established before the failure. It would also be possible that, some time after the control plane failure, the data plane also fails thus causing a complete node failure and a disruption of the established connections through that node.

It is of major importance to establish some mechanisms in order to recover the functionality of the failed control component as soon as possible and re-synchronise the control and forwarding components. This can be achieved by nodes implementing re-synchronisation mechanisms like Non-Stop Forwarding and Graceful Restart [34,35]. This is not easy to accomplish and may take some time due to a first stage of reinstalling or rebooting the control component and the necessary procedures and protocol messages for that re-synchronisation [10].

The issue of resilience of the control plane in GMPLS networks is attracting some attention. In [36], time related signalling parameters are studied to optimise fault detection and control overhead in optical rings. The impact of RSVP-TE and OSPF-TE message loss (i.e., messages for signalling and routing) is studied in [37]. The analytical model presented in [38] can be used to quantify the number of links required in the control plane topology so that the probability of losing a connection set-up or tear down is below some value.

Unlike the above-referenced papers, in this work we address the scenario in which failures can propagate, through the GMPLS control plane from one node to its neighbours, and once the control plane functionality is affected, it is possible that the data plane is affected as well thus creating the two-dimensional failure propagation scenario discussed in the introduction. We focus on optical ring networks for two reasons: First, they are widely deployed as part of several transport technologies and are commonly found in metropolitan area networks [15,39]. Second, their structure lend itself amenable to the study of the evolution of failures and the effects on reliability through continuous-time Markov chains, as will be discussed in the following sections.

2.3. Failure propagation based on epidemic models

Considering that the failures of interest in this paper are those that propagate, epidemic models can be used to characterise the dynamics of the spreading of failures. The term "epidemic network" has been used to describe and study how an epidemic evolves on a set of individuals during a certain amount of time, both in contact networks of biological individuals and in computer networks (see for example [40,41] and the references therein). The rise and decline of an epidemic may be probabilistically characterised, and definitely depends upon the infection propagation rate and the node connection degree [42]. 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 its effects. Examples of networking applications where epidemic network models may apply include power supply networks, social networks, neural networks or computer networks.

A large number of epidemic models have been proposed to characterise the propagation of viruses in complex systems, mainly biological. A good review can be found in [43]. In this paper, we assume that failures propagate according to the SID model recently published by the authors in [44], and described in 2.2. Such studies presented a simulation-based study of the robustness of mesh topologies under the risk of SID based failures. This work completes [44] providing the analytical study of SID on ring topologies, and provides design rules for the repair rates required to achieve a given service availability goal.

3. The SID (Susceptible-Infected-Disabled) model

This section defines the states associated to each node, and the implications of being in each state from the functional point of view. Additionally, the assumptions made about failure spontaneous generation and propagation, necessary for developing the CTMC model in the next section, are also given.

- The S state, 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 to becoming infected (i.e. suffering a failure) if at least one of its neighbours is already infected. Additionally, the node may fail spontaneously, which means that the node is creating a new infection.
- The I state stands for "infected state". In this case, the GMPLS control plane is faulty, but the forwarding plane continues working properly. The node cannot participate in the establishment of new LSPs nor it is able to modify the current configuration of its LSPs. However, the traffic of already active LSPs may still be forwarded. A node in this state may propagate errors to its neighbours.
- The D state stands for "disabled state". In this case, both the control and forwarding planes are faulty. Error propagations to adjacent cannot occur since node communication is disrupted.

Fig. 2 shows the state-transition diagram for the SID model, where the values on the arrows refer to the transition rates between states (the number of transition events that occur per unit of time). Essentially, Fig. 2 states that a node susceptible to being infected (a node that is working properly, i.e. on state S) becomes infected at rate β (if there exists at least one neighbouring 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, β_F refers to the spontaneous failure rate at which a given node in the network, whose neighbours are not infected, may actually become (spontaneously) infected. The rate value of β_F is much smaller than β, so it does not

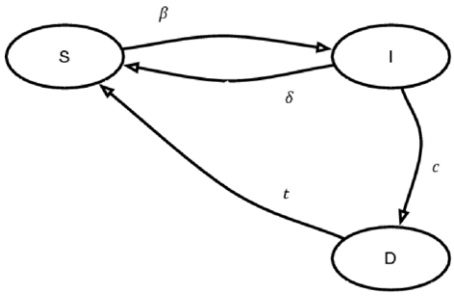


Fig. 2. State-transition-rate diagram for the SID model.

Table 1
Summary of notation and parameters of the SID model.

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

appear in the calculation of the corresponding infection rate for simplicity but also because we are considering the following behavioural hypothesis: when one node has just had a control plane failure (infection), no more isolated nodes are allowed to have control plane failures spontaneously, but rather only by infection propagation. Table 1 summarises the parameters of the SID model.

It is important to remark that, in this scenario, the epidemic spreading of failures happens only among entities of the control plane, that is, the inter-plane failure propagation (from the control plane to the data plane) is not epidemic, rather it is the consequence of assuming that a certain proportion of nodes in the "infected" state cannot be repaired (returned to the "susceptible" state), at which point the data plane (the whole node, in fact) also fails.

4. Analysis

4.1. Continuous-time Markov chain (CTMC) model

In this work, failure events in an individual node are assumed to occur independently from one another and to exhibit the memoryless property, which means that inter-failure times are exponentially distributed. This behaviour is assumed for all possible events that may occur in the scenario: control plane failures (infection propagation), data plane failures (node disabled), control plane repairs and complete node repairs (becoming operational from the disabling state). Then, the use of a continuous-time Markov chain to model the propagation of failures along the GMPLS ring is very suitable. Basically, continuous-time Markov chains (CTMC) are easily characterised by the so-called *state-transition-rate diagram* (Fig. 2), which is a graph showing the system's possible states, along with directed arcs that represent the transition rates (in failure or repair events per unit of time) between states. In this section, we use a CTMC whose states represent all the failure situations that could possibly occur in a GMPLS ring of eight nodes.

Additionally, the model's transition rates between states are related to the failure propagation rates in the SID model of Fig. 2.

The state-transition-rate diagram gives the infinitesimal generation matrix Q, which characterises the transient behaviour of the CTMC. In this work, the matrix Q will be used to study the steady-state probabilities (that is, the percentage of time that the ring is in a given configuration in the long run) and the first-passage times of a given state (that is, the amount of time on average to reach a given state from some other).

Essentially, with Q, the steady-state solution for a CTMC requires solving p_i from the following set of equations:

$$p_i Q_i = \sum_{j \neq i} Q_{ij} p_j, \quad i \in C \tag{1}$$

where

$$\sum_{j \in C} p_j = 1 \tag{2}$$

and

$$Q_i = -\sum_{j \neq i} Q_{ij} \tag{3}$$

where p_i is the steady-state probability of state i, C is the state space and Q_{ij} is the transition rate from state i to state j, as specified in matrix Q. The values of p_i give the amount of time that, in the long run, the CTMC stays on each state. Additionally, the Q matrix allows the computation of the expected transition time between any two nodes of the Markov chain. The first-passage time from state i to state k (hereafter m_{ik}) is the mean time to reach state k for the first time given that the process started in state i, and is computed solving the following set of equations:

$$m_{ik} = \frac{1}{Q_i} + \sum_{j \neq k} \frac{Q_{ij}}{Q_i} m_{jk}, \quad i, j, k \in C \tag{4}$$

where $Q_i = \sum_{j \neq i} Q_{ij}$.

4.2. An eight-node ring study case

Fig. 3 shows an eight-node GMPLS ring network to be modelled by a CTMC. The CTMC model is based on the following assumptions:

(1) Already infected nodes may infect only neighbouring nodes. Basically, a node may be infected only if it has at least one neighbouring node already infected. The first infection occurs spontaneously (β_F).
(2) Already infected nodes may become disabled. Disabled nodes cannot infect other nodes, nor can they propagate their disabling state to other nodes.
(3) Both infected and disabled nodes may be repaired by the administrator, but only if they are adjacent to a susceptible node. In other words, node repair strategies occur at the edges of the infected/disabled area.

In light of this, Fig. 4 shows the complete state-transition-rate diagram of a CTMC model for the ring topology shown in Fig. 3. Each state is labelled with the triple $(N_{ll} : N_D : N_{lr})$, where N_D refers to the number of disabled nodes (nodes in state D), and the N_{ll} and N_{lr} side denotes the number of infected nodes (nodes in state I) on the two sides of the disabled node. When $N_D = 0$ (that is, no nodes are in state D), then the state notation may be reduced to $(0 : 0 : N_{lr})$. For instance, state $(0 : 1 : 1)$ denotes the case of one disabled and one infected node next to the disabled one, regardless of their absolute position in the ring (by convention $N_{ll} \leq N_{lr}$).

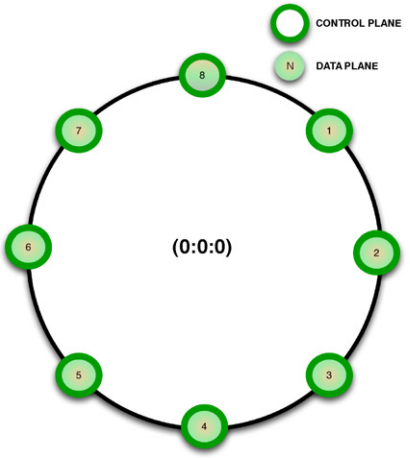


Fig. 3. The eight-node GMPLS-based ring example.

As an example, consider the ring of Fig. 3. Initially, the ring is in state $(0 : 0 : 0)$ as there is no node in either the infected or disabled state. This is illustrated in Fig. 5(a). At some point in time, one node becomes spontaneously infected as depicted in Fig. 5(b). This occurs at rate $8\beta_F$ and brings the ring to the state $(0 : 0 : 1)$. From there on, the infected node may cause the transition to:

- the state $(0 : 1 : 0)$ if it becomes disabled which occurs at rate c. This case is illustrated in Fig. 5(c).
- the state $(0 : 0 : 2)$ if the infection is passed on to a neighbour. This occurs at rate 2β (See Fig. 5(d)) because the infected node may infect either of two neighbouring nodes.
- the state $(0 : 0 : 0)$ (Fig. 5(a)), if the network operator repairs the node and returns it to the susceptible state. The rate of this transition is δ, which is the repairing rate.

Taking a closer look at the state $(0 : 0 : 2)$, we can see that the possible transitions from there on are:

- to the state $(0 : 0 : 3)$ when an additional adjacent node becomes infected (see Fig. 5(e)), which again occurs at rate 2β.
- to the state $(0 : 1 : 1)$ if one of the two infected nodes become disabled, which occurs at rate $2c$ (see Fig. 5(f)).
- to the state $(0 : 0 : 1)$ if one of the two infected nodes is repaired. This occurs at rate 2δ (see Fig. 5(b)).

In contrast, from state $(0 : 1 : 0)$, no new infections develop because disabled nodes do not propagate infection. Therefore, the only possible transition is to the state

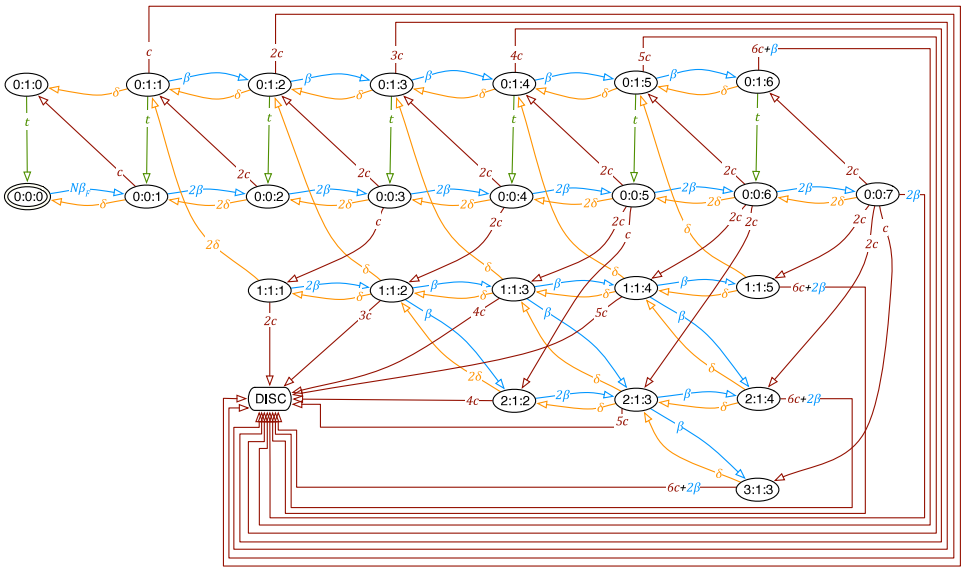


Fig. 4. State-transition-rate diagram for the SID model of an eight-node GMPLS ring.

$(0:0:0)$ when repairing actions are taken by the network operator.

The remaining states and transition rates can be easily computed, thus yielding Fig. 4. In the figure, there is a special state denoted as "DISC". This state comprises a set of many states: All states with more than one disabled node (that is, $x:D:y$ for $D>1$ and any values of x and y) and all states with no susceptible nodes (that is $0:0:8$ and $0:1:7$). Such a "Disconnection" state represents the case where the network operator must take urgent repair action. We consider that the network operator is capable of restoring a disconnected network at rate t_R. The value of t_R is considered to be much smaller than t in order to take into account that "Disconnected" networks are much harder to repair. Finally, the goal of this study is to design the repair rates δ and t to have the ring in the "Disconnection" state less than 99.999% of the time.

Table 2 shows the infinitesimal generation matrix Q_8 for this particular CTMC, as obtained from the state-transition-rate diagram of Fig. 4. The empty gaps are zeros, excepting the diagonal values:

$$Q_{ii} = \sum_{j \neq i} Q_{ij}.$$

4.3. A general model for GMPLS rings with N nodes

From the case with eight nodes, it is easy to infer the following rules in constructing the infinitesimal generation matrix Q_N as it is shown in Table 2, for a ring with a general number of nodes N. These rules are summarised in Table 3.

5. Numerical results

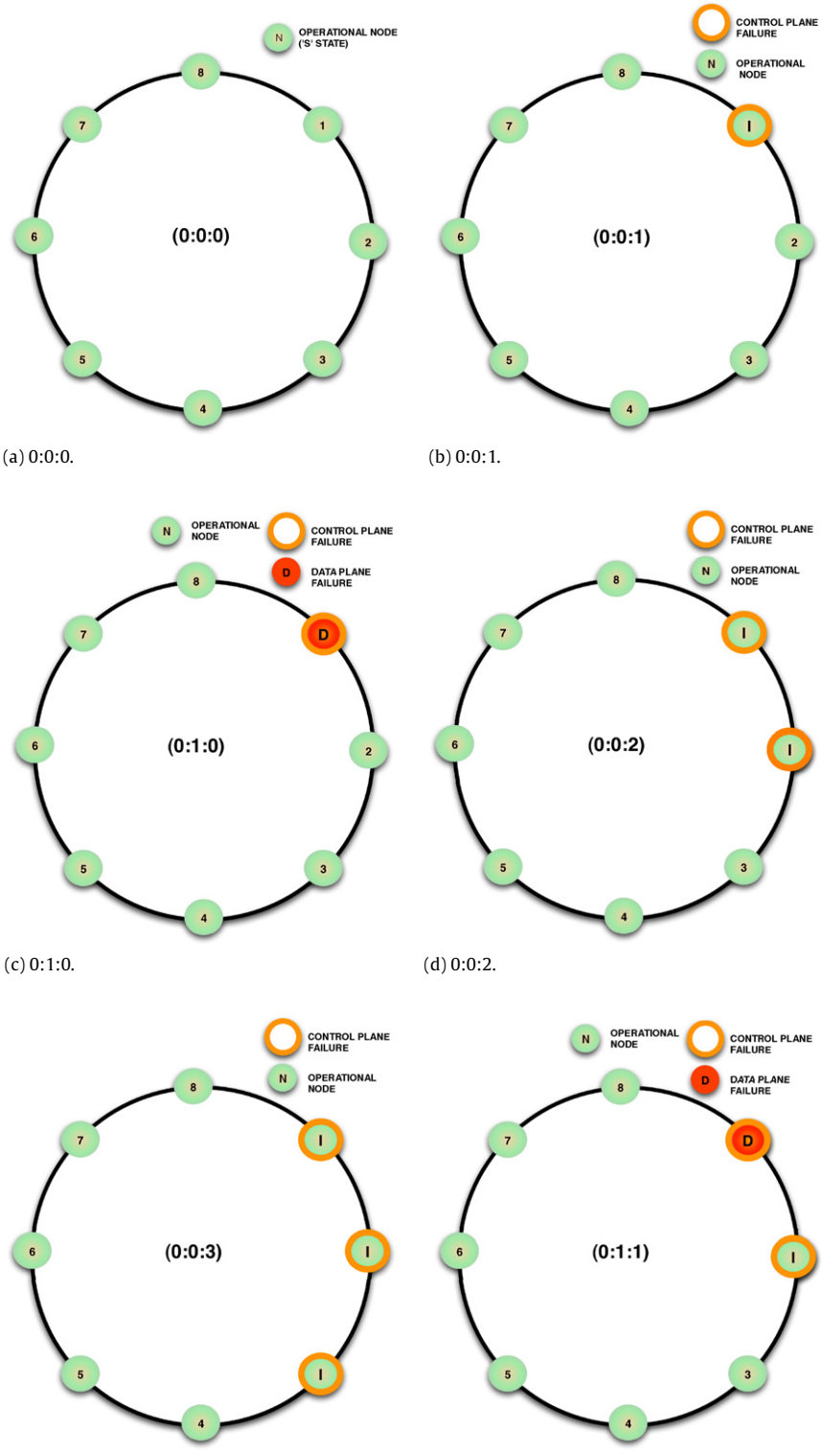
5.1. Performance metrics

Next, we study the steady-state probability of a number of key sets of states in the CTMC, which represent different types of network malfunctioning (see Fig. 6). Such key states are:

- Fully Operational, $(0:0:0)$ state: This is the state at which all nodes in the ring work properly, but are susceptible to spontaneous infection. It is characterised by $P_{(0:0:0)}$, that is, the percentage of time at which the ring has all its nodes fully functional.
- Moderate Infection, $(0:\{0,1\}:< N_{I,\max})$ state: This set contains all the states of the ring where the number of infected nodes is smaller than some value $N_{I,\max}$, and the number of disabled nodes is either 0 or 1. This case is characterised by $P_{low,I}$ which is the sum of the steady-state probabilities of all states meeting such a condition. This group of states refer to a moderate infection propagation along the ring and should be considered by the administrator as a potential case of severe network infection.
- Severe Infection, $(0:\{0,1\}:> N_{I,\max})$ state: This set contains all the states of the ring where the number of infected nodes exceeds some value $N_{I,\max}$, and the number of disabled nodes is either 0 or 1. This case is characterised by $P_{high,I}$, the sum of the steady-state probabilities meeting such a condition. This group of states refers to a severe infection propagation along the ring and should be considered by the network operator as the previous stage towards network disconnection.
- Disconnection, $(DISC)$ state: this is the state in which the ring has more than one disabled node, or all its nodes are infected. In such a case, there are at least two nodes that cannot communicate with each other, which is unacceptable to most network operators. This case is characterised by P_{DISC}, that is, the percentage of time at which the ring has two or more disable nodes, or all the ring nodes are infected.

The value of $N_{I,\max}$ may be chosen between 0 and N. In the numerical examples we use $N_{I,\max} = N/2$, that is, we consider that the severe infection state begins when at least 50% of nodes in the ring have some kind of failure.

Such groups of states are shown in Fig. 6. The "Fully Operational" state is marked using a pentagonal



(a) 0:0:0.

(b) 0:0:1.

(c) 0:1:0.

(d) 0:0:2.

(e) 0:0:3.

(f) 0:1:1.

Fig. 5. Different ring states: (a) (0:0:0), (b) (0:0:1), (c) (0:1:0), (d) (0:0:2), (e) (0:0:3) and (f) (0:1:1).

Table 2
Infinitesimal generation matrix for an eight-node GMPLS ring (Q_8).

Q_8	0:0:0	0:0:1	0:0:2	0:0:3	0:0:4	0:0:5	0:0:6	0:0:7	0:1:0	0:1:1	0:1:2	0:1:3	0:1:4	0:1:5	0:1:6	1:1:1	1:1:2	1:1:3	1:1:4	1:1:5	2:1:2	2:1:3	2:1:4	3:1:3	DISC
0:0:0		$N\beta_F$																							
0:0:1	δ		2β						c																
0:0:2		2δ		2β						$2c$															
0:0:3			2δ		2β						$2c$					c									
0:0:4				2δ		2β						$2c$					$2c$								
0:0:5					2δ		2β						$2c$					$2c$			c				
0:0:6						2δ		2β						$2c$					$2c$			$2c$			
0:0:7							2δ								$2c$					$2c$			$2c$	c	2β
0:1:0	t																								
0:1:1		t							δ		β														c
0:1:2			t							δ		β													$2c$
0:1:3				t							δ		β												$3c$
0:1:4					t							δ		β											$4c$
0:1:5						t							δ		β										$5c$
0:1:6							t							δ											$6c+\beta$
1:1:1										2δ							2β								$2c$
1:1:2											δ					δ		β			β				$3c$
1:1:3												δ					δ		β			β			$4c$
1:1:4													δ					δ		β			β		$5c$
1:1:5														δ					δ						$6c+2\beta$
2:1:2																	2δ					2β			$4c$
2:1:3																		δ			δ		β	β	$5c$
2:1:4																			δ			δ			$6c+2\beta$
3:1:3																						2δ			$6c+2\beta$
DISC																									

Table 3
Transition generation rules for Q_N.

Ring state			
From	To	Q_{ij}	Condition
$(0:0:0)$	$(0:0:1)$	$N\beta_F$	
$(0:0:1)$	(0:1:1)	0	
$(0:1:x)$	$(0:1:x+1)$	β	$x>0$
$(y:1:x)$	$(y:1:x+1)$	β	$x\geq y, y\geq 0$
$(y:1:x)$	$(y+1:1:x)$	β	$x\geq y, y\geq 0$
$(0:0:x)$	$(0:0:x+1)$	2β	$x\geq 1$
$(x:1:x)$	$(x:1:x+1)$	2β	$x\geq 0$
$(0:0:N-1)$	DISC	2β	
$(0:0:x)$	$(0:1:0)$	c	$x\geq 1$
$(0:0:x)$	$(\frac{x-1}{2}:1:\frac{x-1}{2})$	c	x odd and $x\geq 2$
$(0:0:x)$	$(0:1:x-1)$	2c	$x\geq 1$
$(0:0:x)$	$(y:1:x-y-1)$	2c	$y=1,2,3,\ldots$ *while* $y\leq x$
$(y:0:x)$	DISC	$(x+y)c$	
$(0:1:N-2)$	DISC	$(N-2)c+\beta$	
$(y:1:N-y-2)$	DISC	$(N-2)c+2\beta$	
$(0:1:x)$	$(0:0:x)$	t	
$(0:0:1)$	$(0:0:0)$	2δ	
$(x:1:x)$	$(x-1:1:x)$	2δ	$x\geq 1$
$(0:0:x)$	$(0:0:x-1)$	δ	$x\geq 2$
$(y:1:x)$	$(y:1:x-1)$	δ	$x>y$
$(y:1:x)$	$(y-1:1:x)$	δ	$x>y>0$

shape. States belonging to the "Moderate Infection" group use square-shaped boxes while "Severe Infection" ones are surrounding by an elliptical shape. Finally the "Disconnection" is clearly marked with a rounded-corner rectangle.

Additionally, it is of interest to study the average first-passage times to any of the three malfunctioning groups of states to see how often these situations arise from a fully functional state $(0:0:0)$.

The following numerical examples study these performance metrics in detail.

5.2. Steady-state probability results

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 set of states as a function of the two repairing rates: the rate δ, at which the control

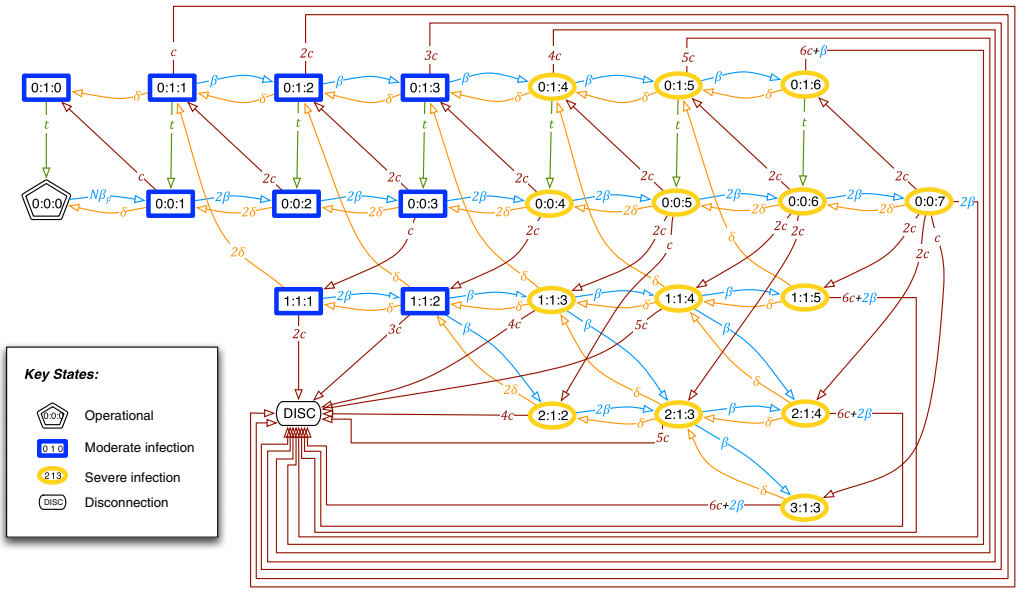


Fig. 6. Groups of states under study.

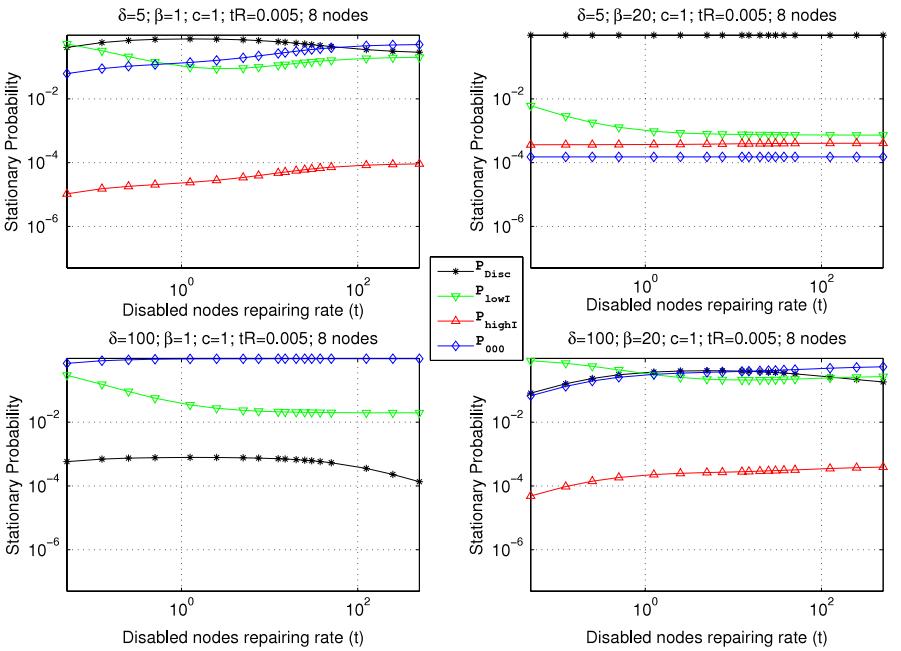


Fig. 7. Impact of t on the steady-state probabilities of the CTMC for the eight-node GMPLS ring.

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). The units of all the rates are normalised as the amount of transitions events (failures or reparations) that occur in an infinitesimal period of time in the CTMC model.

Numerical results are plotted for different values of δ, β, t and c. The figures use the following notation: Subindex "000" is used for the Fully Operational state, subindex "HighI" represents the Severe Infection case, "LowI" is used for Moderate Infection results and finally "DISC" here refers to the Disconnection state results.

Fig. 7 shows the steady-state probabilities of the CTMC for the eight-node GMPLS ring for different values of δ, β, c and t. The control and data plane repair rate value is fixed at $c = 1$ repair per unit of time (e.g. hour) for all four plots. The two upper plots consider $\delta = 5$ (control plane repair rate) while the two lower plots consider $\delta = 100$. The two plots on the left consider a fixed value of $\beta = 1$ (infection rate), while the two plots on the right consider a fixed $\beta = 20$ value. Several conclusions arise from this figure: First,

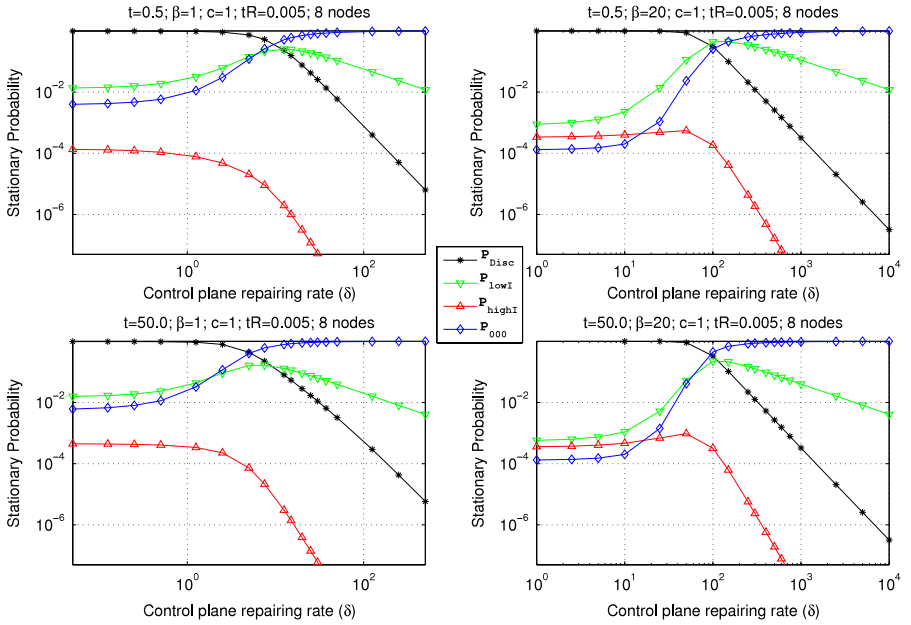


Fig. 8. Impact of δ on the steady-state probabilities of the CTMC for the eight-node GMPLS ring.

the four scenarios show an almost constant steady-state probability, regardless of the value of t (almost horizontal lines). Second, the upper-left and lower-right figures have the same $\beta/\delta = 1/5$ ratio and show very similar steady-state probabilities. Only the bottom-left plot of Fig. 7 shows a reasonably low P_{DISC} value, which has a $\beta/\delta = 1/100$ low value. Essentially, the ratio β/δ is the key in having a sufficiently low value of P_{DISC} as shown in Fig. 8.

Fig. 8 considers the value of $t = 0.5$ (top plots) and $t = 50$ (bottom plots) for different infection rates $\beta = 1$ (left plots) and $\beta = 20$ (right plots). The plots show similar behaviour with decreasing disconnection probability P_{DISC} for large values of δ for different values of β. Essentially, in order to achieve a disconnection steady-state probability below 10^{-5}, $\delta > 4 \times 10^2\beta$ when $\beta = 1$ is required (Fig. 8 top- and bottom-right) and $\delta > 4 \times 10^3\beta$ when $\beta = 20$ (Fig. 8 top- and bottom-left). Hence, it is safe to have a repairing rate δ about three orders of magnitude larger than the infection rate β, i.e. $\delta > 10^3\beta$ to guarantee 99.999% network availability.

5.3. First-passage times: MTTF and MTTR

This section studies the first-passage times of the three malfunctioning groups of states: Moderate infection, Severe infection and Disconnection, starting from state $(0:0:0)$. This is referred to as Mean Time To Failure (MTTF) as it gives the average time to reach each state starting from the fully operational state $(0:0:0)$, as computed from Eq. (4).

As shown in Fig. 9, the behaviour is again independent of t (upper and lower figures look the same). Again, the message is that, in order to have a failure after 10^5 units of time, the value of δ must be large enough in comparison with β, that is of about three orders of magnitude larger.

Finally the Mean Time To Repair (MTTR) analysis is shown in Fig. 10. This figure gives the average time required to get to state $(0:0:0)$ from any of the malfunctioning groups of states. In order to achieve very low MTTR values (in the order of 10^{-2} units of time), the values of δ are required to be several orders of magnitude larger than β.

5.4. A GMPLS ring with 32 nodes

This section shows numerical results for a large-size ring of 32 nodes. Using the rules inferred in Section 4.3, the infinitesimal generation matrix Q_{32} is calculated and hence the steady-state probabilities for the CTMC model are resolved for the 32-node ring. Fig. 11 shows the ratio δ/β (y-axis) required to achieve a certain service unavailability (x-axis), assuming different combinations of β and t. As shown, for a desired service unavailability of 10^{-5} the value of δ must be between 10^2 and 10^3 times the value of β. This conclusion was also obtained from the analysis of the eight-node ring of the previous section. This provides a rule for network operators in the design of their δ value strategy.

6. Summary and conclusions

This work has presented a CTMC model to characterise the transient behaviour and possible states of GMPLS-based networks with ring topology whose nodes may become infected or disabled following the SID failure propagation model. A full set of numerical examples has been presented, focused on analysing the resulting steady-state probabilities along with the Mean Time To Failure and Mean Time To Repair values for a selected number of δ and t repair rates on two GMPLS rings of 8 and 32 nodes, respectively.

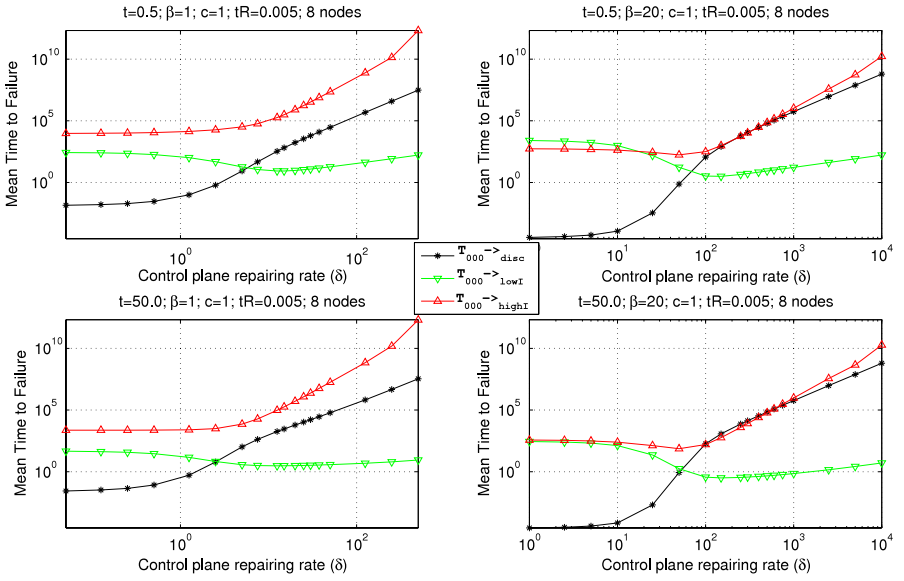


Fig. 9. Mean time to failure (MTTF) results.

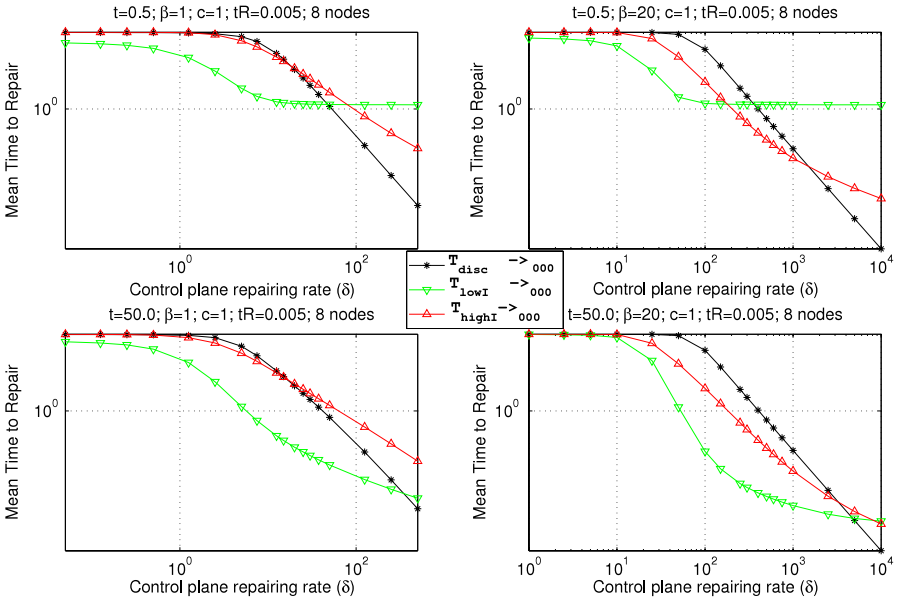


Fig. 10. Mean Time To Repair (MTTR) results.

The presented CTMC model can help network operators in finding the required repair rates of control and data planes δ and t to maintain a certain level of availability, say 99.999%. Additionally, the model can be used 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 of the SID model (Susceptible, Infected or Disabled).

As it is concluded from the numerical examples conducted with rings of different sizes, a good design rule is to have the repair rate of infected nodes δ much larger (about three orders of magnitude) than the infection rate β. Basically, when δ is so large with respect to β we have infected nodes which are repaired very quickly, minimising the probability of infecting others.

This is clearly seen from the next example: When the CTMC moves from state $(0:0:0)$ to state $(0:0:1)$, then the next movement is either to $(0:0:2)$, $(0:1:0)$ or back $(0:0:0)$, with rates 2β, c and δ respectively. By keeping $\delta \gg (2\beta + c)$, the network operator ensures that the infection propagates to neighbouring nodes with very little probability, only:

$$\frac{2\beta}{2\beta + \delta + c}.$$

Hence, the network operator must ensure that $\delta \gg \beta$ in order to avoid infection propagation.

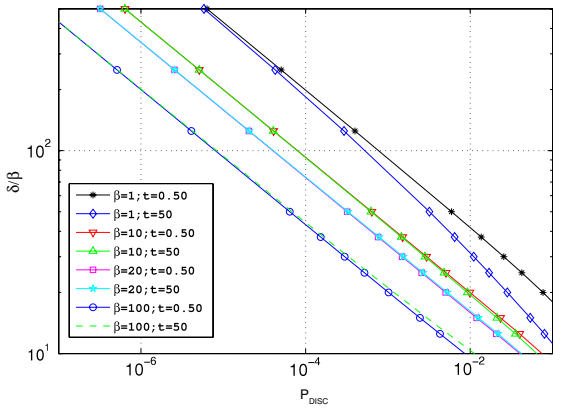


Fig. 11. Impact of δ/β in the steady-state probabilities of the CTMC for the 32-node GMPLS ring.

Acknowledgements

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

Additionally, the authors would like to thank the support of the T2C2 Spanish project (under code TIN2008-06739-C04-01) and the CAM-UC3M Greencom research grant (under code CCG10-UC3M/TIC-5624) in the development of this work.

References

[1] J.P. Sterbenz, D. Hutchison, E.K. Çetinkaya, A. Jabbar, J.P. Rohrer, M. Schöller, P. Smith, Resilience and survivability in communication networks: strategies, principles, and survey of disciplines, Computer Networks 54 (8) (2010) 1245–1265.

[2] A. Haider, R. Harris, Recovery techniques in next generation networks, IEEE Communications, Surveys and Tutorials 9 (3) (2007) 2–17.

[3] M. Pickavet, P. Demeester, D. Colle, D. Staessens, B. Puype, L. Depre, I. Lievens, Recovery in multilayer optical networks, Journal of Lightwave Technology 24 (1) (2006) 122–134.

[4] E. Mannie, Generalized Multi-Protocol Label Switching (GMPLS) Architecture, RFC 3945 (Proposed Standard) (Oct. 2004). URL: http://www.ietf.org/rfc/rfc3945.txt.

[5] M. Vigoureux, B. Berde, L. Andersson, T. Cinkler, L. Levrau, M. Ondata, D. Colle, J. Fernandez-Palacios, M. Jager, Multilayer traffic engineering for GMPLS-enabled networks, IEEE Communications Magazine 43 (7) (2005) 44–50.

[6] P. Demeester, M. Gryseels, K.V. Doorselaere, A. Autenrieth, C. Brianza, G. Signorelli, K. Van, M. Ravera, C.B. Italtel, G.S. Sirti, R. Clemente, M.R. Cselt, A. Jajszczyk, D.J. Itti, G.K. Belgacom, Y. Harada, S.O. Ntt, A.G.R. Int, C.P. Demeester, Resilience in a multi-layer network, IEEE Communications Magazine 37 (1999) 70–76.

[7] P. Cholda, A. Jajszczyk, Recovery and its quality in multilayer networks, Lightwave Technology, Journal of 28 (4) (2010) 372–389.

[8] A. Jajszczyk, P. Rozycki, Recovery of the control plane after failures in ASON/GMPLS networks, IEEE Network 20 (1) (2006) 4–10.

[9] A. Farrel, I. Bryskin, GMPLS: Architecture and Applications, Morgan-Kaufmann (Elsevier), 2004.

[10] G. Li, J. Yates, D. Wang, C. Kalmanek, Control plane design for reliable optical networks, IEEE Communications Magazine 40 (2) (2002) 90–96.

[11] O. Crochat, J.-Y. Le Boudec, O. Gerstel, Protection interoperability for WDM optical networks, IEEE/ACM Transactions on Networking 8 (3) (2000) 384–395.

[12] M. Kurant, P. Thiran, Survivable routing of mesh topologies in IP-over-WDM networks by recursive graph contraction, IEEE Journal on Selected Areas in Communications 25 (5) (2007) 922–933.

[13] C. Liu, L. Ruan, A new survivable mapping problem in IP-over-WDM networks, IEEE Journal on Selected Areas in Communications 25 (3) (2007) 25–34.

[14] K. Thulasiraman, T. Lin, M. Javed, G. Xue, Logical topology augmentation for guaranteed survivability under multiple failures in IP-over-WDM optical networks, Optical Switching and Networking 7 (4) (2010) 206–214.

[15] A. Narula-Tam, E. Modiano, A. Brzezinski, Physical topology design for survivable routing of logical rings in WDM-based networks, IEEE Journal on Selected Areas in Communications 22 (8) (2004) 1525–1538.

[16] A. Jaekel, S. Bandyopadhyay, Y. Aneja, Logical topology design for WDM networks using survivable routing, in: IEEE International Conference on Communications, 2006. ICC'06, vol. 6, 2006, pp. 2471–2476.

[17] P. Pacharintanakul, D. Tipper, The effects of multi-layer traffic on the survivability of IP-over-WDM networks, in: ICC'09: Proceedings of the 2009 IEEE International Conference on Communications, IEEE Press, Piscataway, NJ, USA, 2009, pp. 2354–2359.

[18] K. Lee, E. Modiano, Cross-layer survivability in WDM-based networks, in: IEEE INFOCOM 2009, 2009, pp. 1017–1025.

[19] S. Huang, M. Xia, C. Martel, B. Mukherjee, A multistate multipath provisioning scheme for differentiated failures in telecom mesh networks, Journal of Lightwave Technology 28 (11) (2010) 1585–1596.

[20] J. Zhang, B. Mukherjee, A review of fault management in WDM mesh networks: basic concepts and research challenges, IEEE Network 18 (2) (2004) 41–48.

[21] J. Doucette, W. Grover, Capacity design studies of span-restorable mesh transport networks with shared-risk link group (SRLG) effects, in: SPIE Optical Networking and Communications Conference, Opticomm 2002, vol. 4874, Citeseer, 2002, pp. 25–38.

[22] L. Shen, X. Yang, B. Ramamurthy, Shared risk link group (SRLG)-diverse path provisioning under hybrid service level agreements in wavelength-routed optical mesh networks, IEEE/ACM Transactions on Networking (TON) 13 (4) (2005) 918–931.

[23] D. Coudert, F. Huc, F. Peix, M. Voge, Reliability of connections in multilayer networks under shared risk groups and costs constraints, in: IEEE International Conference on Communications, 2008. ICC'08, IEEE, 2008, pp. 5170–5174.

[24] G. O'Reilly, A. Jrad, R. Nagarajan, T. Brown, S. Conrad, Critical infrastructure analysis of telecom for natural disasters, in: Telecommunications, Network Strategy and Planning Symposium, 2006. NETWORKS 2006. 12th International, 2006, pp. 1–6.

[25] Y. Kitamura, Y. Lee, R. Sakiyama, K. Okamura, Experience with restoration of Asia Pacific network failures from Taiwan earthquake, IEICE Transactions 90-B (11) (2007) 3095–3103.

[26] M. Lesk, The new front line: estonia under cyberassault, IEEE Security and Privacy 5 (2007) 76–79.

[27] R. Albert, H. Jeong, A.-L. Barabasi, Error and attack tolerance of complex networks, Nature 406 (6794) (2000) 378–382.

[28] L. Zhao, K. Park, Y.-C. Lai, Attack vulnerability of scale-free networks due to cascading breakdown, Physical Review E 70 (3) (2004) 035101.

[29] C. Magnien, M. Latapy, J.-L. Guillau, Impact of random failures and attacks on Poisson and power-law random networks, ACM Comput. Surv. 43 (3) (2011) 13:1–13:31.

[30] T. Bilski, Disaster's impact on internet performance–case study, in: A. Kwiecień, P. Gaj, P. Stera (Eds.), Computer Networks, in: Communications in Computer and Information Science, vol. 39, Springer, Berlin, Heidelberg, 2009, pp. 210–217. URL: http://dx.doi.org/10.1007/978-3-642-02671-3_25.

[31] E. Coffman, Z. Ge, V. Misra, D. Towsley, Network resilience: exploring cascading failures within BGP, in: Allerton Conference on Communication, Control and Computing, 2002.

[32] S. Neumayer, G. Zussman, R. Cohen, E. Modiano, Assessing the vulnerability of the fiber infrastructure to disasters, in: INFOCOM, 2009, pp. 1566–1574.

[33] S. Neumayer, E. Modiano, Network reliability with geographically correlated failures, in: Proceedings IEEE INFOCOM, 2010, 2010, pp. 1–9.

[34] K. Nguyen, B. Jaumard, A. Agarwal, A distributed and scalable routing table manager for the next generation of IP routers, IEEE Network 22 (2) (2008) 6–14.

[35] A. Capello, S. Milani, C. Moriondo, G. Rossi, P. Salamandra, M. Perrone, M. Barone, Non-stop forwarding behaviour and performance in high-end ip routers for isp's backbone networks, in: 5th International Workshop on Design of Reliable Communication Networks, 2005, DRCN 2005. Proceedings., 2005, pp. 279–285.

[36] J. Perello, S. Spadaro, J. Comellas, G. Junyent, An analytical study of control plane failures impact on GMPLS ring optical networks, IEEE Communications Letters 11 (8) (2007) 695–697.
[37] O. Komolafe, J. Sventek, Impact of GMPLS control message loss, Journal of Lightwave Technology 26 (14) (2008) 2029–2036.
[38] M. Ruiz, J. Perello, L. Velasco, S. Spadaro, J. Comellas, An analytical model for GMPLS control plane resilience quantification, IEEE Communications Letters 13 (12) (2009) 977–979.
[39] J.M. Finochietto, J. Aracil, Ángel Ferreiro, J.P.F.-P. Giménez, Óscar González de Dios, Migration strategies toward all optical metropolitan access rings, Journal of Lightwave Technology 25 (8) (2007) 1918–1930.
[40] A. Ganesh, L. Massoulie, D. Towsley, The effect of network topology on the spread of epidemics, in: INFOCOM 2005, IEEE, vol. 2, 2005, pp. 1455–1466.
[41] D. Chakrabarti, Y. Wang, C. Wang, J. Leskovec, C. Faloutsos, Epidemic thresholds in real networks, ACM Transactions on Information Systems Security 10 (4) (2008) 1–26.
[42] M. Barthélemy, A. Barrat, R. Pastor-Satorras, A. Vespignani, Dynamical patterns of epidemic outbreaks in complex heterogeneous networks, Journal of Theoretical Biology 235 (2) (2005) 275–288.
[43] T.G. Lewis, Network Science: Theory and Applications, Wiley Publishing, 2009.
[44] E. Calle, J. Ripoll, J. Segovia, P. Vilá, M. Manzano, A multiple failure propagation model in GMPLS-based networks, IEEE Network 24 (6) (2010) 17–22.