A Multiple Failure Propagation Model in GMPLS-Based Networks

Eusebi Calle, Jordi Ripoll, Juan Segovia, Pere Vilà, and Marc Manzano, University of Girona

Abstract

In this article, a new model to simulate different failure propagation scenarios in GMPLS-based networks is proposed. Several types of failures and malfunctions may spread along the network following different patterns (hardware failures, natural disasters, accidents, configuration errors, viruses, software bugs, etc.). The current literature presents several models for the spreading of failures in general networks. In communication networks, a failure affects not only nodes but also the connections passing through those nodes. The model in this article takes into account GMPLS node failures, affecting both data and control planes. The model is tested by simulation using different types of network topologies. In addition, a new method for the classification of network robustness is also introduced.

Multiple failures in a network can occur due to different situations, such as cascading failures due to natural disasters or a virus/worm attack. In order to characterize the dynamics of a multiple failure spreading from a single node to the whole network, epidemic models can be used.

Epidemic networks is a general term that describes how an epidemic spreads when new cases of a certain disease, in a given population and during a given period, substantially exceed what is expected based on recent experience. The rise and decline in epidemic prevalence of an infectious disease is a probability phenomenon dependent on the transfer of an effective dose of the infectious agent from an infected individual to a susceptible one. Research in this area involves different aspects, such as modeling how an epidemic evolves or how to immunize part of the population to minimize or control the effect of the epidemic. Power supply networks, social networks, neural networks, and computer networks are some cases where this subject is of special relevance. Furthermore, it is possible to generalize from viruses (or diseases) to failures, in terms of propagation over a network.

An epidemic network can be modeled as a set of nodes and links representing how the epidemic (the failure propagation) could evolve. Several types of nodes (or individuals) and failures can be represented. For instance, in a medical context when a failure affects a node, it refers to a biological virus infecting a cell. In power supply networks, a failure refers to a power station stopping providing service. There are few proposals modeling the behavior of an epidemic in transport networks. Currently, major proposals focus on single network failures. Moreover, multiple failure proposals are not studied in depth in a failure propagation environment. The main problem in transport networks is that a failure not only affects a node but also a chain of nodes (a path). This is not taken into account in current major epidemic models. In the literature there are only a few proposals focusing on wireless networks [1]. In this article, as an innovation, we focus on failure propagation models for networks based on generalized multiprotocol label switching (GMPLS). In GMPLS, flows are connection-oriented and information is routed along label switched paths (LSPs). Our aim is to provide a model to study the behavior of these failures occurring in these specific types of transport networks.

In optical transport networks based on a GMPLS control plane, failures can occur in both data and control planes. Depending on the functionality of a failed element, failures can be divided into two groups: control plane failures, which make services unmanageable, and data plane failures, which directly affect services. For instance, failures range from a fiber being cut to cross-connects, amplifiers, dense wavelength-division multiplexing (DWDM) devices, network controllers, and control channels going out of service unexpectedly. This article refers specifically to failures that propagate over the network, affecting both data and control planes in a substantial number of nodes.

The remaining sections have the following structure. The next section gives a background of previous work in epidemic models. GMPLS-based network failures are then explained. We then describe our proposed model. The simulation scenario is then presented, and the article concludes in the final section.

Epidemic Models: Related Work

The problem of virus propagation has attracted huge interest among the scientific community. There are several families described in the literature dealing with models of virus propagation. The first family, called 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 can be used for *worst case propagation*. Another family is the Susceptible-Infected-Susceptible (SIS) group, which considers that a susceptible individual can become infected on contact with another infected individual, then recovers with some likelihood of becoming susceptible again. Therefore, individuals will change their

 0890-8044/10/$25.00

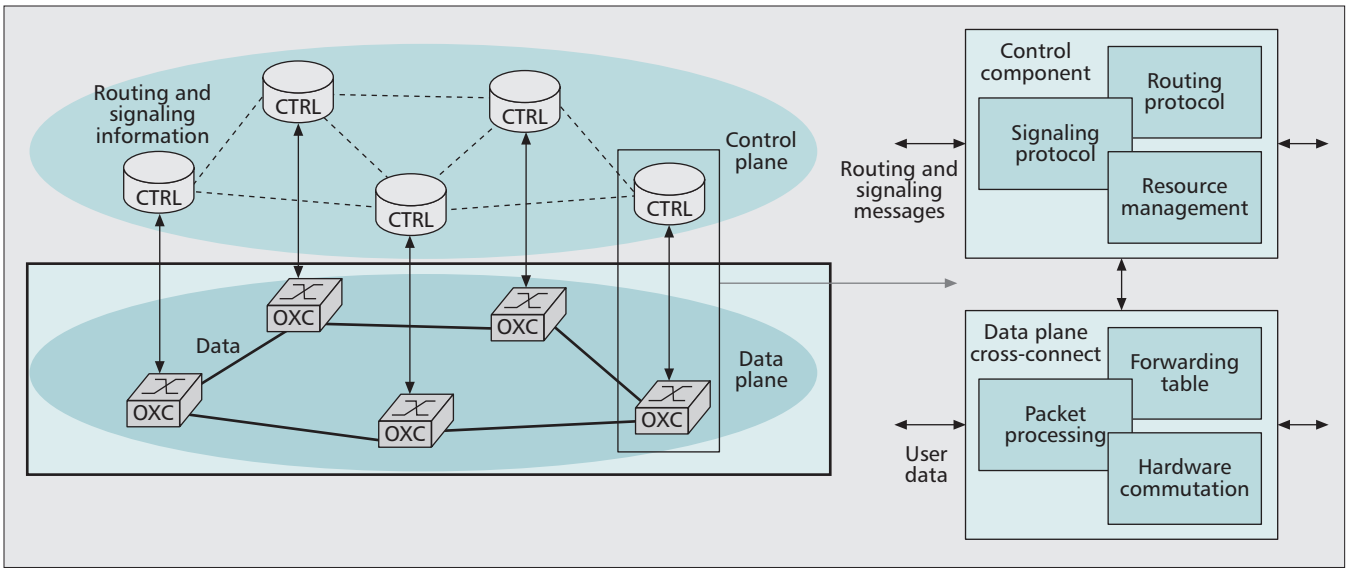

Figure 1. *The control and data planes in the GMPLS architecture.*

state from susceptible to infected, and vice versa, several times. The third family is 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: Susceptible-Infected-Detected-Removed (SIDR) and Susceptible-Infected-Removed-Susceptible (SIRS). The first one adds a Detected (D) state, and is used to study virus throttling, which is an automatic mechanism for restraining or 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 and then goes back to the susceptible state.

There are several proposed models included in the SIS family. Kephart and White (KW) [2] were among the first to propose epidemiology-based models to analyze the propagation of computer viruses. In their model, the communication among individuals is modeled as a directed graph: a directed edge from node i to node j denotes that i can directly infect j. A rate of infection, called the birth rate, is associated with each edge. A virus death rate (also called the node curing rate) is associated with each infected node.

The KW model provides a good approximation of virus propagation in networks where contact among individuals is sufficiently homogeneous. However, a crucial point to be taken into account in epidemics is the network topology. A network topology can be characterized using different topology parameters, such as node degree, diameter, number of nodes/links, degree distribution functions, clustering features, and so on. Based on these features, a classification of different network topologies can be established: homogeneous, random, small-world, power law, and scale-free topologies, among others. In [3] a detailed characterization of them can be found. For instance, it is assumed that the Internet resembles a scale-free topology, where some nodes are highly connected (high node degree), while the majority of the nodes are not. Nowadays, major real networks (including social networks, router, and autonomous system [AS] networks) follow a power-law structure. Communication networks are usually modeled as scale-free [4]. In this article, for devising the epidemic model as well as performing the simulations to test it, a set of representative topologies of communication networks have been selected.

Currently, several epidemic models have been proposed considering different network topologies and dynamics. For instance, [1] proposes a model for wireless networks. However, to the best of our knowledge, no epidemic model exists for optical communication networks. As a novelty, in this article we present a new model based on an optical GMPLS-based network.

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 and signaling protocols. 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 (Fig. 1) it is possible that some attack or failure could occur that affects only the control plane. If this is the case, the routing and signaling 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 not be dropped (i.e., the data plane continues working properly).

If a node is attacked by a virus or there is a bad software configuration, it can happen that only a specific function in the control plain fails [6]. For instance, if the signaling 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 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 signaling 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 article it is assumed that a control plane failure always involves both signaling and routing modules, so as to reduce the number of failure scenarios.

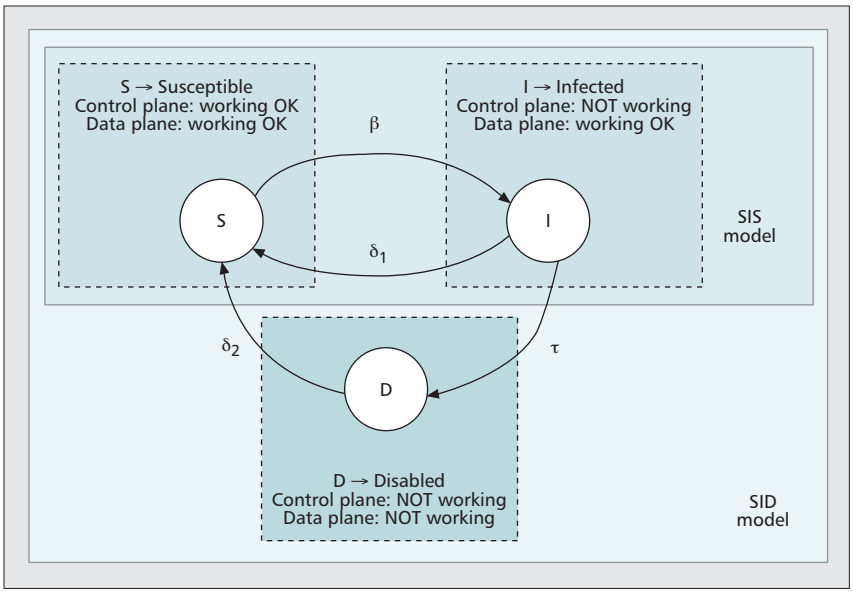

Figure 2. *State diagram of the SIS and SID models and the relationship to the operational status of the GMPLS planes.*

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 resynchronize 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 resynchronization [6]. It is also necessary that nodes implement resynchronization 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.

The SIS and SID Models

In this section, the application of the well-known SIS model to GMPLS-based networks is presented. The main difference between the SIS model in other research areas and in communications networks is that in the latter the infection of a node affects not only that node but also the paths crossing it. In order to overcome that limitation of the SIS model in GMPLS-based networks, an extension model called SID (Susceptible, Infected, and Disabled), is introduced.

Figure 2 shows the state diagram of the SIS model, as seen from a single node. Each node, at each time-step t, is either susceptible (S) or infected (I). A susceptible node that is currently not infected can be infected with probability β by receiving the infection from a neighbor. An infected node can be repaired with probability δ_1. In a GMPLS-based network a node being in the state (I) means that in that node the control plane is failing, and consequently, no new connections can be attended by this node. It is interesting to note that the larger the $1 - \delta_1$, the larger the number of path requests blocked by this node. δ_1 can be evaluated by taking into account the time to detect the failure and the time to repair (and sometimes update) the modules affected by the failure/virus attack. This process can be performed without disrupting the ongoing connections in the data plane.

In order to consider a more realistic scenario, an extension of the SIS model, called here Susceptible-Infected-Disabled (SID), is introduced. More precisely, we have constructed and analyzed an SID model as an extension of the SIS model for connected undirected networks described in [7]. Figure 2 also shows the state diagram of the SID model and its relation to SIS. Each node of the network can be in one of three states: *susceptible* (uninfected), *infected*, or *disabled*. The *disabled* state takes into account the fact that an infected node could degrade to complete nodal failure (i.e., control and data plane failure). When a node becomes disabled, all connections crossing that node are removed. In that case, the node needs a process to be repaired, and the time needed is directly proportional to the mean time to repair (*MTTR*). So, in our model δ_2 can be computed as $1/MTTR$. It is worth mentioning that in this model an infected node is not necessarily repaired, which is a notable difference with the previous reviewed models.

Our model is described by a *Markov chain* in either continuous time or discrete time with a small enough time step. We have computed the *basic reproduction number*, usually denoted R_0, defined as the average number of infections produced by an infective individual (infected node) in a wholly susceptible population (network). We have that

$$R_0 = \frac{\beta}{\delta_1 + \tau}\lambda_1$$

(we refer to [8] for R_0 in a wide range of models), where $\lambda_1 > 0$ is the largest eigenvalue of the non-negative irreducible symmetric adjacency matrix of the network. For the particular case of a homogeneous network, the largest eigenvalue is equal to the average nodal degree [7, 9]. The formula for R_0 above can be interpreted as follows: $\beta\lambda_1$ is the transmission rate across an infective contact times the expected number of contacts (connexions), whereas

$$\frac{1}{\delta_1 + \tau}$$

gives the expected lifetime of an infected node (i.e., the mean infectious period).

Therefore, the following epidemic threshold can be stated:

- If $R_0 < 1$, equivalently,

$$\frac{\beta}{\delta_1 + \tau} < \frac{1}{\lambda_1};$$

  then the infection dies out over time, that is, the number of infected and disabled nodes goes to zero.
- If $R_0 > 1$, equivalently,

$$\frac{\beta}{\delta_1 + \tau} > \frac{1}{\lambda_1};$$

  then there is an epidemic outbreak affecting ultimately a fraction of the network nodes.

It can be pointed out that the spread of the infection in the network depends on the topology of the network through the single parameter $\lambda_1 > 0$. This phenomenon follows on from the systematic approach of considering the linearization of the model around the disease-free steady state, where the adjacency matrix of the network appears and its largest eigenvalue λ_1 determines the (un)stability. Analogous results have been reported in [7, 9] for the case of the SIS model.

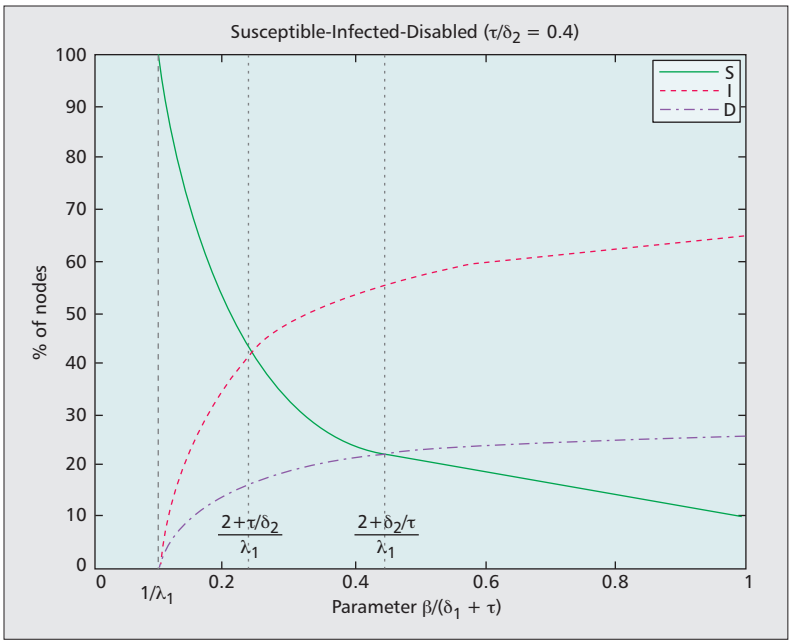

Figure 3. *SID model: analytical values for the number of nodes per state.*

Finally, for a homogeneous network we have explicit expressions for the endemic steady state. The fraction of susceptible nodes is $1/R_0$, the fraction of infected nodes is

$$\left(1-\frac{1}{R_0}\right)\frac{1}{1+R_1} \text{ with } R_1=\frac{\tau}{\delta_2},$$

and the fraction of disabled nodes is

$$\left(1-\frac{1}{R_0}\right)\frac{R_1}{1+R_1}.$$

Figure 3 shows these proportions varying the parameter $\beta/(\delta_1 + \tau)$. Moreover, this endemic equilibrium is asymptotically stable whenever it exists ($R_0 > 1$).

Figure 3 shows analytically the values for the number of nodes in the susceptible, infected, and disabled states following the model presented in this section. Two important points are highlighted in the figure: the intersection of the infected and susceptible curves, and the intersection of the disabled and susceptible curves. The mathematical expressions for both intersection points of our model are also given.

Simulations and Discussion

In this section, the simulations performed to test the SID model are presented, and a new measure to assess the robustness against epidemics in communication networks is introduced.

Validation of the SID Model

In order to validate the analytical SID model presented in the previous section, simulations were performed to observe the evolution of an epidemic outbreak on a GMPLS-based network.

Different network topologies are considered in the simulations, which are chosen to be as heterogeneous as possible, and, according to [4], trying to be representative of a communication network. Heterogeneity is achieved by selecting different topology parameters, such as nodal degree, average diameter, and so on. A different node degree distribution has also been taken into account for the network selection. Some of these features are summarized in Table 1, including the largest eigenvalue. In the simulations, requests arrived according to a Poisson distribution with exponentially distributed holding times. Source and destination are randomly selected.

Considering the aim of the simulations (i.e., to test the model), a specific epidemic scenario is set up by choosing the probabilities δ_1, δ_2, β, and τ. For instance, in Fig. 4a these values are $\delta_1 = 0.3$, $\delta_2 = 0.3$, $\tau = 0.1$, and $\beta = 0.167$. The expected fraction of infected nodes is

$$\left(1-\frac{1}{R_0}\right)\frac{1}{1+R_1} \text{ with } R_1=\frac{\tau}{\delta_2},$$

so the analytical value is 37.5 percent. As can be seen in the figure, once the epidemic reaches the steady state, the fraction of infected nodes is close to the analytical value. Similarly, values for the number of susceptible and disabled nodes can be obtained. Several simulations have been performed to confirm that the analytical and simulation values are always equal.

A New Measure of Robustness against Epidemics in GMPLS Networks

When a new connection request is rejected because some required resource is not available, it is said to be blocked (i.e., no LSP is allocated for it). Blocking will also result in a GMPLS-based network as a consequence of nodes entering the infected state, as defined earlier. In this simulation it is assumed that resources, such as capacity, are always available, and no other path quality constraint is imposed (e.g., maximum hop count, delay). Thus, the blocking ratio only depends on the effects of the epidemic.

A topology can be considered *more robust* than another one if the same epidemic spreads more slowly on it than on the other. In the literature, one of the most commonly used robustness metrics is the *largest eigenvalue*, where the larger this value, the more robust the topology [7]. However, that approach has an important drawback when applied to communication networks (e.g., GMPLS): it relies solely on the topology's adjacency matrix, and thus the connections/LSPs carried by the network are not taken into account.

Given that it is possible to generate an infection of equivalent level in different topologies thanks to the mathematical model presented earlier, the behavior of each topology can be observed and compared. More specifically, if two GMPLS-

Feature	T204	T65	T400
Average nodal degree	3.21	3.32	3.75
Diameter	18	8	19
Avg. shortest path length	7.82	3.91	9.06
Largest eigenvalue	3.803	4.789	5.195
Number of nodes	204	65	400
Number of links	652	108	749

Table 1. *Main features of the topologies.*

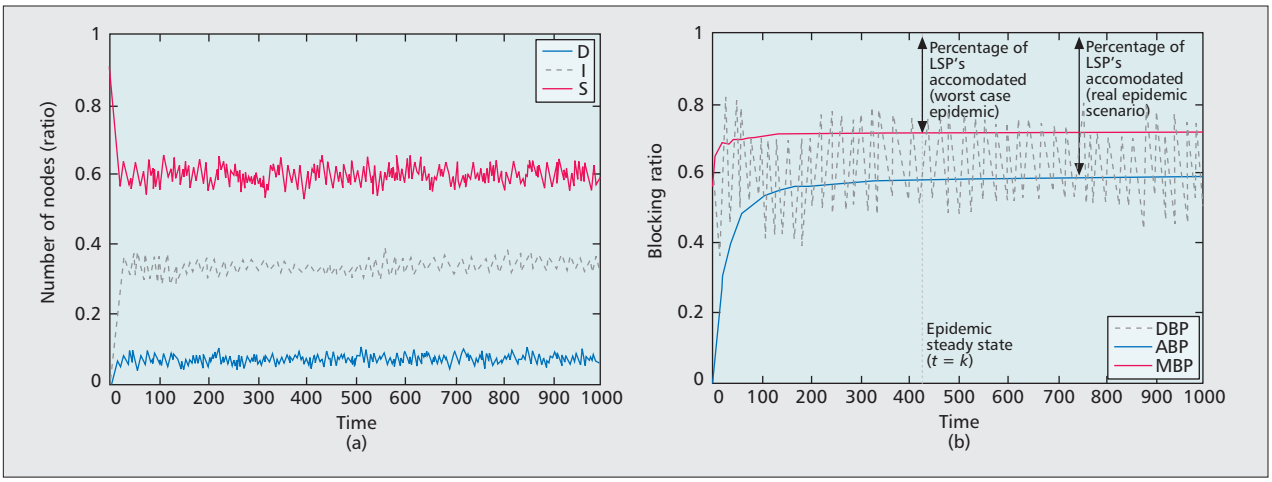

Figure 4. *Epidemic spreading on the T65 topology when $\delta_1 = 0.3$, $\delta_2 = 0.3$, $\tau = 0.1$, and $\beta = 0.167$: a) evolution of the number of nodes per state; b) ABP, DBP, and MBP.*

based networks are subject to exactly the same epidemic, the infection's speed in reaching the steady state is an indication of the networks' robustness. In order to measure this speed, it is possible to observe the connection blocking evolution; that is, if the infection spreads fast, more nodes become infected, and consequently, more requests are blocked. We call this measure the *topology robustness against epidemics in GMPLS networks*, or TRG.

Figure 4b can help us to clarify the relation of TRG with connection blocking and also define it more formally. This figure shows the temporal evolution of the blocking ratio. At that any discrete simulated time t, a certain number (Q_t) of new connection requests arrive. Some of them (B_t) are rejected due to the epidemic effects. This instantaneous blocking ratio is B_t/Q_t, identified as DBP in the figure. The global blocking ratio, that is, the blocking that corresponds to the whole period from time 0 up to time t, is $\sum_{i=0}^{t}(B_i/Q_i)$, identified in the figure as accumulated blocking probability (ABP).

As our interest is in evaluating the impact of the speed of the epidemic, we can additionally observe what happens to the blocking ratio when the network is subject to the worst possible infection scenario from the beginning, that is, when the number of infected nodes is already the maximum since time 0. If the epidemic evolves to the worst case slowly, the topology is more robust; consequently, more connections will be accommodated. This is shown in Fig. 4b as maximum blocking probability (MBP).

TRG can be formally defined as the area between ABP and MBP, once the epidemic reaches its steady-state at $t = k$, that is, TRG $= \int_{t=0}^{k}(MBP - ABP)dt$. The larger the area, the more robust the topology. As MBP and ABP are accumulated values, a simple approximation is the difference between them.

By comparing the TRG of different topologies, and considering the same epidemic level, we can identify the most robust one. This is shown in Fig. 5, where the TRGs for the three topologies are depicted under different infection levels, which are defined by assigning several values to R_0. Table 2 shows the values of MBP, ABP, and TRG for the three topologies under an extreme infection level. As can be seen, according to the TRG, the most robust topology is T65, as its TRG is more than two times that of T400 and more than three times that of T204. If we ranked the topologies according to their largest eigenvalue, as in [7], the most robust topology would be T400, followed by T65 and T204.

Contrary to the measure based on largest eigenvalue, with TRG it is also possible to observe that the topologies perform differently when the epidemic scenarios change. For instance, T65 outperforms the others under light and extreme infections, but it is not the best in the rest of the cases. This behavior can be explained by the fact that TRG considers not only the speed of the epidemic but also the connections path lengths. Note that the probability of a connection being rejected is higher as its path length increases. As can be seen in Table 1, T65 has much shorter average path lengths than the others, and its largest eigenvalue is in between the other two.

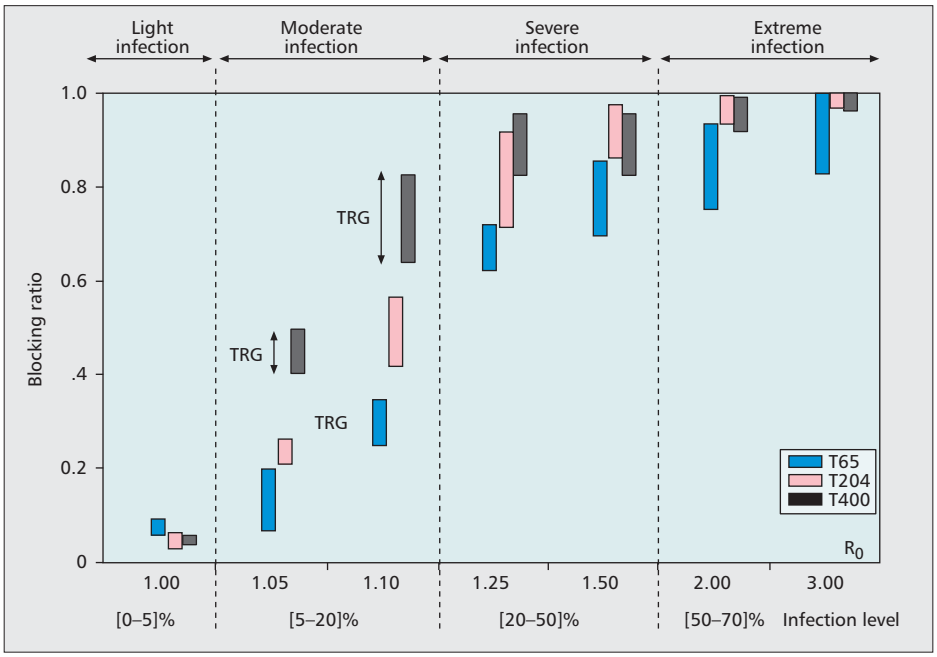

Figure 5. *Robustness comparison of the three studied topologies under different epidemic scenarios, based on blocking ratio.*

Topology	MBP	ABP	TRG	λ
T204	0.9967	0.9395	0.0572	3.803
T65	0.9292	0.7457	0.1835	4.789
T400	0.9946	0.9140	0.0806	5.195

Table 2. *Comparison of TRGs at an extreme infection level ($R_0 = 2.00$).*

Therefore, as shown in this section, the presented SID model can be used to define different epidemic scenarios, and measure the robustness of the underlying topologies by using TRG.

Conclusions

In this article, a new model for the study of the spreading of failures in GMPLS-based networks has been proposed. In order to define our model, a review of the existing epidemic and failure propagation models has been presented, highlighting the limitations of such models to represent some aspects of practical importance in telecommunication networks. To study the effect of epidemic failures on already established paths, this new model, called SID (for Susceptible-Infected-Disabled), assigns a state to partial node failures, which happens when a failing node is able to retain certain functionality, whereby existing LSPs can survive the failure. Complete node failures are represented by the *disabled* state. The mathematical formulation for finding the epidemic threshold has also been given.

In order to evaluate the performance of our model, extensive simulations have been carried out on different network topologies. The results show an excellent match between the estimation of the evolution of the epidemic as predicted by the analytical model and the values obtained through simulation. Moreover, a new metric for assessing and comparing the robustness of networks to epidemic failures has been discussed, together with numerical examples applied to the studied topologies. This metric, which we call TRG, offers insight into the performance of a network topology at different infection levels in terms of blocking ratio. Therefore, it can prove to be more useful in networking than other measures based purely on topological features such as the largest eigenvalue.

Acknowledgments

This work is partially supported by Spanish Ministry of Science and Innovation project TEC 2009-10724 and MTM 200806349-C03, and by the Generalitat de Catalunya research support program SGR-1202 and SGR-345.

References

[1] S. Tang and B. Mark, "Analysis of Virus Spread in Wireless Sensor Networks: An Epidemic Model," *7th Int'l. Wksp. Design of Reliable Commun. Net.*, Oct. 25–28, 2009, pp. 86–91.
[2] J. O. Kephart and S. R. White, "Directed-Graph Epidemiological Models of Computer Viruses," *Proc. IEEE Symp. Security Privacy*, 1991, p. 343.
[3] T. G. Lewis, *Network Science: Theory and Applications*, Wiley, 2009.
[4] A. L. Barabasi, "The Architecture of Complexity," *IEEE Control Sys.*, vol. 27, no. 4, 2007, pp. 33–42.
[5] A. Jajszczyk and P. Rozycki, "Recovery of the Control Plane after Failures in ASON/GMPLS Networks," *IEEE Network*, vol. 20, no. 1, Jan./Feb. 2006, pp. 4–10.
[6] G. Li *et al.*, "Control Plane Design for Reliable Optical Networks," *IEEE Commun. Mag.*, vol. 40, no. 2, Feb. 2002, pp. 90–96.
[7] D. Chakrabarti *et al.*, "Epidemic Thresholds in Real Networks," *ACM Trans. Info. Sys. Security*, vol. 10, no. 4, 2008, pp. 1–26.
[8] O. Diekmann and J. A. P. Heesterbeek, *Mathematical Epidemiology of Infectious Diseases: Model Building, Analysis, and Interpretation*, 1st ed., Wiley, May 2000.
[9] R. Pastor-Satorras and A. Vespignani, "Epidemic Dynamics in Finite Size Scale-Free Networks," *Physical Rev. E*, vol. 65, no. 3, paper no. 035108, Mar. 2002.

Biographies

EUSEBI CALLE (eusebi@eia.udg.edu) is an associate professor at the University of Girona (UdG), where he received his doctorate degree in computer science in 2004. Since 1998 he has been a member of the research and teaching staff of the Broadband Communications and Distributed System Group at the UdG, where he develops his research in GMPLS fault management, routing, and network science. He has co-authored several papers in international journals and international conferences. He is also a member of different TPCs, and part of the Institute of Informatics and Applications at the UdG.

JORDI RIPOLL (jripoll@ima.udg.edu) is an associate professor in the Department of Computer Science and Applied Mathematics at the UdG, where he is a member of the research coordinated project entitled Evolution Equations, Complex Networks, and Population Dynamics. He received his Ph.D. degree in mathematical sciences from the University of Barcelona in 2005 and has worked on models of structured population dynamics with special emphasis on models of epidemic spreading in complex networks. He made several postdoctoral research stays and is a co-author of several papers in international journals and conferences.

JUAN SEGOVIA (jsegovia@eia.udg.edu) received his Bachelor's degree in computer science from the National University of Asunción in 1994 and an MPM degree in 2000 from the same university. He is currently a Ph.D. candidate at the Institute of Informatics and Applications of the UdG, and is a member of the Broadband Communications and Distributed Systems group. His research interests include protection and restoration of GMPLS-based optical networks, and reliability against large-scale failures in complex networks.

PERE VILÀ (perev@eia.udg.edu) is a lecturer in the Department of Computer Architecture and Technology at the UdG, where he is a member of the Broadband Communications and Distributed Systems research group. He received his Ph.D. in computer science in 2004. His current research interests are in the fields of network management, routing, and protection, and interdomain mechanisms. He has co-authored several papers in journals and international conferences, and worked on several funded research projects.

MARC MANZANO (mmanzano@eia.udg.edu) is a part time lecturer in the Department of Computer Architecture and Technology at the UdG, where he received his Bachelor's degree in computer science in 2009. Since 2008 he is a member of the Broadband Communications and Distributed Systems research group of the Institute of Informatics and Applications at the UdG, developing his research in routing, protection, and network management.