Abstract—In this paper a survey of the main proposals to simulate in Transport Networks is presented. A new model focused on GMPLS-based networks is proposed. The proposal is evaluated and results show that the model is able to simulate different failure propagation scenarios. Results also offer identifying what are the critical parts of the network when a failure propagation occurs in order to protect and minimize the impact of a failure.

Index Terms—Epidemic Networks, Survivability, Network Models, GMPLS.

I. INTRODUCTION

Epidemic networks is a general term that describes how an epidemic occurs 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 upon 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 a part of the population to minimize or control the effect of the epidemic. Power supply networks, social networks, neural networks or computer networks are some cases where this subject is of special relevance. Furthermore, it is possible to generalize from virus (or diseases) to failures, in terms of propagation over a network.

A network can be modeled as a node (representing individuals) 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. As well as when, in power supply networks, a failure refers to a power station stopping providing service.

There is a few proposals modeling the behavior of an epidemic (a failure propagation) in transport networks. Currently, major proposals focus on single network failures. Moreover, multiple failures proposals are not studied in a failure propagation environment. In the literature only few proposals focus on wireless networks are investigated [1]. In this paper, as a novelty, we focus on failure propagation models for networks based on Generalized Multi-Protocol Label Switching (GMPLS) [2]. 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 this specific type of transport networks.

In optical transport networks, based on a GMPLS control plane, failures can occur in both data/control plane. Depending on the functionality of a failed element, failures can be divided into two groups: control plane failures, that make services unmanageable, and data plane failures, that directly affect services. For instance, failures include from a fiber getting cut to cross-connects, amplifiers, DWDM devices, networks controllers, and control channels going out of service unexpectedly. This paper 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. II gives a background review of previous work. In III, we describe our proposed model. In IV, the accuracy of our results is demonstrated by experiments carried out under several conditions. Conclusions are presented in section V.

II. RELATED WORK

The problem of virus propagation has attracted huge interest among the scientific community. There are several families described in the literature involving models of virus propagation. 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, for this reason, can be used for “worst case propagation”. In the second place, there is the Susceptible-Infected-Susceptible (SIS) group, which considers a susceptible individual can become infected on contact with another infected individual, then recovers with some probability to become susceptible again. Therefore, individuals will 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 removal state. In the SIR group, an individual can be infected just once because when the infected individual recovers from the disease, it will get some immunity and it will not pass the infection onto others anymore. Finally there are two families that extend the SIR one: 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, which is an automatic mechanism for restraining or slowing the spread of diseases. The second one considers that after an individual becomes removed, it remains in that state for an specific period and then change its state to susceptible again.

There are several proposed models included in the SIS family. The classification given in Table I shows for what kind of network topologies these models have been devised.

### TABLE I
**Classification of Different Types of Network Structures**

<table>
<thead>
<tr>
<th>Network Structure</th>
<th>Main Features</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Homogeneous Networks</td>
<td>Individual, have equal contact to others in the population and the rate of infection is largely determined by the density of the infected population.</td>
<td>[3] [4]</td>
</tr>
<tr>
<td>Barabási-Albert (BA) power-law topology</td>
<td>Major nodes have a low node degree.</td>
<td>[5] [6] [7]</td>
</tr>
<tr>
<td>Mean Field approximation in power-law topologies</td>
<td>All graphs with a given distribution degree are considered equal.</td>
<td>[6]</td>
</tr>
<tr>
<td>Highly clustered power-law topologies</td>
<td>More realistic behavior than power-law topologies with random wiring.</td>
<td>[8]</td>
</tr>
<tr>
<td>Correlated Networks</td>
<td>The connectivity of a node is related to the connectivity of its neighbours. These correlated networks include Markovian networks.</td>
<td>[9]</td>
</tr>
<tr>
<td>Generic, Meshed Networks</td>
<td>No constraints about the network topology.</td>
<td>[10]</td>
</tr>
<tr>
<td>Ad-hoc networks</td>
<td>Individuals can be in constant movement. Dynamic topologies.</td>
<td>[1]</td>
</tr>
</tbody>
</table>

Kephart and White [3] [4] 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 $\beta$, called the birth rate, is associated with each edge. A virus death rate $\delta$ (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 the contact among individuals is sufficiently homogeneous. However, there is overwhelming evidence that real networks (including social networks, router and AS networks and Gnutella overlay graphs) deviate from such homogeneity [11] [12] [13]; they follow a power-law structure instead, which means that there exist a few nodes with a very high connectivity, but the majority of the nodes have low connectivity. Pastor-Satorras and Vespignani studied viral propagation for Barabási-Albert (BA) [14] power-law topology [5] [6] [7]. Unfortunately, this model does not hold for many real networks [15] [12]. Several follow-up attempts focus on analyzing even more realistic graph models. Eguiluz and Klemm [8] obtain accurate results on several graphs representing major properties of Internet. A more precise and general than previous models is presented in [10], called the Non Linear Dynamic System (NLDS) model. This model demonstrate its accuracy in networks with no constraints about the topology.

Since the models presented in this section are classified into the SIS group, all of them consider that a node will always be repaired. However, a fundamental feature of an operational transport network is that an infected node must have a process to be repaired and that this process does not necessarily has to finish successfully. Consequently, a new model should be defined to mimic the desired behavior.

### III. Extending Failure Propagation Models to GMPLS-based Networks

In this section an overview of the NLDS model is presented and a new one is proposed, called the Susceptible-Infected-Disabled (SID) model, is introduced. It is based on the NLDS model due to its topology independence and its aim is to provide an optimum model ready to work with GMPLS networks.

#### A. The NLDS model

In this section the NLDS [10] model is presented.

![Fig. 1. State diagram of the NLDS model](Image)

This model works with small discrete time-steps $\Delta t$, with $\Delta t \to 0$. Fig. 1 shows the state diagram of the NLDS 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 $\beta$ by receiving the virus from a neighbor. An infected node can be repaired with probability $\delta$.

#### B. The Susceptible-Infected-Disabled (SID) model

The Susceptible-Infected-Disabled (SID) model extends the model illustrated in III-A with one state as it aims to represent the behavior of individuals in GMPLS-based networks. A new state is introduced, called disabled (D). This new state represents the fact that an infected node needs a process to
be repaired. This process could be instantaneous, take a big amount of time or never stop. Therefore, an infected node does not necessarily be always repaired. Accordingly, our model is composed of three states:

- The S state (also called SUSCEPTIBLE state).
- The I state (also called INFECTED state).
- The D state (also called DISABLED state).

Our new model could seem to be a member of the SIRS family. Nevertheless, it is not because models that belong to that family are designed to repair every individual after being removed, and in our model, an individual may not be repaired after that.

![Fig. 2. A node divided functionally in two: Control and Data plane.](image)

In a network administered by GMPLS, nodes are divided functionally into two, in response to the needs of Control and Data plane of GMPLS. Fig. 2 shows both parts. Consequently, depending on the state in which a node can be, abilities such as LSP creation, LSP destruction or signaling among others, are assigned to a node:

- When a node is susceptible, it is working properly (so it can create and delete LSP if it has not got a neighbor that is either infected or disabled). Therefore, this node has both layers working.
- When a node is infected, the lower part of the Fig. 2 is still working. However, the upper part of the router (the Control Plane) is impaired. Consequently, the node ability is reduced to forwarding the existing LSP that were passing through itself before the node became infected.
- When a node is disabled, it has the upper and lower part of the Fig. 2 non-functional. For that reason, the node has no ability to provide any type of service.

Fig. 3 shows the state diagram of the SID model. A susceptible node becomes infected upon contact with another infected individual with probability $\beta$. When a node becomes infected, the repairing process is started. After this process, the node can be repaired with probability $\delta$ (to go back to the S state). If it is not repaired successfully, probability $c$ determines if it becomes disabled (and it goes to D state). If it does not become disabled, the repairing process is started again, and it will remain infected until this process ends. When a node reaches the D state (so it is disabled) another repairing process is started (different from the one in the I state).

**IV. SIMULATION AND ANALYSIS**

In this section simulation results are presented. Simulations are carried out in order to check the suitability of the proposal to model the behavior of an epidemic on any specified topology (unless otherwise specified, each simulation plot is averaged over 15 runs).

Two topologies have been used to perform the evaluation. The topologies are generated using BRITTE [16]. Features of both topologies are listed in Table II.

**TABLE II**

<table>
<thead>
<tr>
<th>Topology FEATURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of nodes</td>
</tr>
<tr>
<td>100</td>
</tr>
<tr>
<td>200</td>
</tr>
</tbody>
</table>

Simulations are carried out using OMNet++ [17]. Simulations start with a set of randomly chosen infected nodes on the given network topology. The set of parameters used in the two evaluations is listed in Table III.

**TABLE III**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>100 nodes</th>
<th>200 nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\beta$</td>
<td>0.085</td>
<td>0.051</td>
</tr>
<tr>
<td>$\delta$</td>
<td>0.05</td>
<td>0.03</td>
</tr>
<tr>
<td>$c$</td>
<td>0.1</td>
<td>0.1</td>
</tr>
<tr>
<td>Time to repair (Infected)</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Time to repair (Disabled)</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Percentage of infected nodes</td>
<td>10%</td>
<td>20%</td>
</tr>
</tbody>
</table>

Requests arrived according to a Poisson distribution and exponentially distributed holding time. Source and destination are randomly selected.

Fig. 4 shows the time evolution of the percentage of nodes that are in each of the states defined in our model. Simulation starts with a 10% of nodes randomly infected. The number of infected nodes stabilizes around time = 20. In this simulation we achieve a stabilized value of 40% of nodes. It is interesting that the infected curve provides a parallel behavior to the disabled curve, as expected in our model.

Fig. 5 shows the number of affected connections per node. This information is useful in order to detect the hot points of the network. These nodes could be protected (immunized) to avoid/minimize the impact of the epidemic.
Fig. 4. Percentage of infected nodes during the simulation with a topology of 100 nodes

Fig. 5. Ranking of nodes that have lost more connections during the simulation with a topology of 100 nodes

Fig. 6 shows and epidemic spreading that begins with a 20% of nodes randomly infected. Around time = 10 the percentage stabilizes around the 10%, while the disabled nodes percentage keeps oscillating between 2% and 5%.

V. CONCLUSION

In this paper a new proposal to model the behavior of a failure propagation is presented. A review of previous models and the challenges to be used in GMPLS-based networks has been also presented.

Finally, some preliminary simulations have shown the suitability of our model in order to simulate different failure propagation scenarios. For future work the addition of new models to immunize the network will be considered.

REFERENCES


