Modelling spreading of failures in GMPLS-based Networks

M. Manzano, J. Segovia, E. Calle, P. Vilà, J. L. Marzo
Institute of Informatics and Applications (IIiA), University of Girona,
Girona 17071, Spain
Email: {mmanzano, jsegovia, eusebi, perev, marzo}@ia.udg.edu

Abstract—In this paper, a new model to simulate different failure propagation scenarios in GMPLS-based networks is proposed. Different types of failures and malfunctions may spread along the network following different patterns (hardware failures, natural disasters, accidents, configuration errors, viruses, software bugs, etc). Current literature presents several models describing how failures could spread throughout the network. However, existing models usually consider failures affecting single nodes instead of connections, as in transport networks. The proposed model also takes into account GMPLS node failures, affecting both data and control planes. This model has been evaluated using exhaustive simulations and several failure propagation scenarios have been identified. These scenarios can be used to develop and evaluate protection / immunization schemes in order to minimize the impact of failures.

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

I. INTRODUCTION

Epidemic networks (EN) is a general term that describes how an epidemic evolves 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 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 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.

An EN 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. Just as when, in power supply networks, a failure refers to when a power station stops 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 failures proposals are not deeply studied 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 major current epidemic models. In the literature there are several proposals focused on wireless networks [1] [2]. In this paper, as an innovation, we focus on failure propagation models for networks based on Generalized Multi-Protocol Label Switching (GMPLS) [3]. 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, that make services unmanageable, and data plane failures, that directly affect services. For instance, failures range from a fiber being 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. Section II gives a background review of previous work. In III, we describe our proposed model. In IV the simulation scenario is presented. In V, the accuracy of our results is demonstrated by experiments carried out under several conditions. Conclusion is presented in section VI.

II. 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 the Susceptible-Infected (SI) considers individuals as being either susceptible (S) or infected (I). This family assumes that the infected individuals will remain infected forever and, so, 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 state...
from susceptible to infected, and vice versa, several times. The third family is the Susceptible-Infected-Removed (SIR), which extends the SI model to take into account the removed state. In the SIR group, an individual can be infected just once because when the infected individual recovers, they become immune and will no longer pass the infection onto others. Finally there are two families that extend the SIR family: SIDR (Susceptible Infected Detected Removed) and SIRS(Susceptible Infected Removed Susceptible). The first one adds a Detected (D) state, and is used to study the virus throttling, which is an automatic mechanism for restraining or slowing down the spread of diseases. The second one considers that after an individual becomes removed, they remain in that state for a specific period and then go back to the susceptible state.

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

TABLE I
CLASSIFICATION OF DIFFERENT TYPES OF NETWORK TOPOLOGIES

<table>
<thead>
<tr>
<th>Network topology</th>
<th>Main features</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Homogeneous topologies</td>
<td>Nodes have equal node degree and the rate of infection is largely determined by the density of the infected population.</td>
<td>[4] [5]</td>
</tr>
<tr>
<td>Power-law topology, Barabási-Albert (BA)</td>
<td>Major nodes have a low node degree.</td>
<td>[6] [7] [8]</td>
</tr>
<tr>
<td>Power-law topologies, Highly clustered models</td>
<td>Power-law topologies considering clusters.</td>
<td>[9]</td>
</tr>
<tr>
<td>Correlated topologies</td>
<td>The connectivity of a node is related to the connectivity of its neighbours. These correlated networks include Markovian networks.</td>
<td>[10]</td>
</tr>
<tr>
<td>Generic topologies, Meshed Networks</td>
<td>No constraints about the network topology.</td>
<td>[11]</td>
</tr>
<tr>
<td>Dynamic topologies</td>
<td>Nodes can be in constant movement.</td>
<td>[1]</td>
</tr>
</tbody>
</table>

Kephart and White (KW) [4] [5] 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 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 [12] [13] [14]. Instead, they follow a power-law structure, whereby there exist a few nodes with very high connectivity, but the majority of nodes have low connectivity. Pastor-Satorras and Vespignani studied viral propagation for Barabási-Albert (BA) [15] power-law topology [6] [7] [8]. Unfortunately, this model does not hold for many real networks [16] [13]. Several follow-up attempts focus on analyzing even more realistic graph models. Eguíluz and Klemm [9] obtain accurate results on several graphs representing major properties of the Internet. A more precise and general model than previous ones is presented in [11], called the Non Linear Dynamic System (NLDS) model. This model demonstrates its accuracy in networks without constraints on 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 main 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 have to finish successfully and so an infected node affects all connections established through it. Consequently, a new model should be defined to mimic these behaviors. The next section takes into account both aspects to extend current models to GMPLS-based networks.

III. EXTENDING FAILURE PROPAGATION MODELS TO GMPLS-BASED NETWORKS

In this section an overview of the NLDS model is presented as a suitable source to develop our own model, and a new one, called the Susceptible-Infected-Disabled (SID) model, is proposed and 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 he NLDS [11] model is presented.

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 infection from a neighbor. An infected node can be repaired with probability $\delta$.  

![State diagram of the NLDS model](image)

Fig. 1. State diagram of the NLDS model
B. The Susceptible-Infected-Disabled (SID) model

The Susceptible-Infected-Disabled (SID) model extends the model described in section III-A by adding one state as it aims to represent the behavior of a node 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 or could take a huge amount of time. Therefore, an infected node is not necessarily repaired -a notable difference to the previous reviewed models. Consequently, our model is depicted by three states:

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

It should be highlighted that our new model could appear to be a member of the SIRS family. Although, it is not due to the fact that these models that belong to that family are assumed that every individual is repaired after being removed. In our model, a node might not be repaired after removal.

In a network, managed by GMPLS, nodes are divided functionally into two, in response to GMPLS control and data plane needs. Fig. 2 shows both parts. Conceptually, both planes work independently. Therefore, the forwarding plane could remain operating even though the control plane may have partial or total impairment. In this work it is assumed when an infection occurs at the control plane, the network operator has the ability to detect this situation and initiate corrective actions. These actions do not always report the node restoration. In this work the following behaviors of nodes are considered:

- When a node is susceptible (S), it is working properly.
- When a node is infected (I), the forwarding plane is still working. However, the control plane fails. Consequently, the node functionality is reduced to forwarding the existing LSPs passing through itself.
- When a node is disabled (D), the forwarding and control plane (Fig. 2) are non-functional and so 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, which lasts $t$ time units. After this time has expired, the node becomes susceptible with probability $\delta$ and disabled with probability $c$ and remains in the infected state with probability $1-\delta-c$, in which case the waiting period of $t$ time units just described is repeated. When a node reaches the disabled state another repairing process is started.

IV. SIMULATION SCENARIO

In this section the simulation tool and the model implementation are presented. The selected topologies are also described.

Two topologies have been used to perform the evaluations defined in section V. The topologies have been generated using BRITE [17]. The first, of 100 nodes, has a diameter of 12 nodes and a mean node degree of 3.08, while the second one, of 200 nodes, has the same diameter but a mean node degree of 3.56. Frequency tables of nodal degrees of both topologies are listed in Table II and Table III.

<table>
<thead>
<tr>
<th>Node degree</th>
<th>Percentage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>28</td>
</tr>
<tr>
<td>3</td>
<td>51</td>
</tr>
<tr>
<td>4</td>
<td>12</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
</tr>
</tbody>
</table>

This work uses the OMNeT++ (Objective Modular Network Testbed in C++) discrete-event simulation platform. OMNeT++ is an object-oriented modular test-bed simulator [18], whereby each module in the network is implemented as an object. Additionally, OMNeT++ supports hierarchically nested modules with flexible module parameters. For our work, we developed components that interact with the INET framework, which is an open-source communication networks simulation package for the OMNeT++ simulation environment. The INET framework contains modules for several Internet protocols,
TABLE III
FREQUENCY TABLE OF NODAL DEGREES OF THE 200-NODE TOPOLOGY

<table>
<thead>
<tr>
<th>Node degree</th>
<th>Percentage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>14</td>
</tr>
<tr>
<td>3</td>
<td>55.5</td>
</tr>
<tr>
<td>4</td>
<td>14.5</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>4.5</td>
</tr>
<tr>
<td>7</td>
<td>1.5</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>0.5</td>
</tr>
<tr>
<td>13</td>
<td>0.5</td>
</tr>
</tbody>
</table>

Fig. 5. 200-node topology

including GMPLS. The following components from the INET framework library have been used:

- RSVP_LSR: Represents the behavior of a RSVP-TE capable router. It consists of a set of submodules such as the TED (*Traffic Engineering Database*), the Routing Table or the MPLS among others.
- RSVP_FAILED: Represents a failed router. It discards all incoming traffic and generates nothing.
- ScenarioManager: This is used for setting up and controlling the simulation experiments. Scheduling of certain events to take place at specified times, like changing a parameter value, changing the bit error rate of a connection, removing or adding connections, removing or adding routes in a routing table can be accomplished.

When a node is in the S or I state, it uses the RSVP_LSR module. However, when it becomes disabled it uses the RSVP_FAILED module. During the simulation, the ScenarioManager has the responsibility of, at each time step, calculating the next state of all nodes, and then updating their possible new state. The SID model behavior has been added as a submodule to the RSVP_LSR and RSVP_FAILED modules. This new submodule has been called RouterState and its duty is to make the simulation of a failure propagation between nodes possible.

V. SIMULATION AND ANALYSIS OF THE SID MODEL

In this section simulation results are presented. Simulations are carried out to check the performance of the proposal to model the behavior of an epidemic on a given topology.

A large number of simulations generating different epidemic scenarios have been carried out. By setting up different values for \( \beta \), \( \delta \) and \( c \), we have been able to achieve an epidemic affecting the whole network, an epidemic completely withdrawn after a period of time, and we have been also able to stabilize the epidemic in a defined percentage.

In this section, some of these scenarios are shown. Simulation starts with a set of randomly chosen infected nodes on the given network topology. The set of parameters used in the four evaluations is listed in Table IV.

TABLE IV
PARAMETERS USED IN THE SIMULATIONS

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Simulation 1</th>
<th>Simulation 2</th>
<th>Simulation 3</th>
<th>Simulation 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of nodes</td>
<td>100</td>
<td>100</td>
<td>200</td>
<td>200</td>
</tr>
<tr>
<td>( \beta )</td>
<td>0.085</td>
<td>0.017</td>
<td>0.085</td>
<td>0.051</td>
</tr>
<tr>
<td>( \delta )</td>
<td>0.05</td>
<td>0.01</td>
<td>0.05</td>
<td>0.03</td>
</tr>
<tr>
<td>( c )</td>
<td>0.1</td>
<td>0.1</td>
<td>0.1</td>
<td>0.1</td>
</tr>
<tr>
<td>Time to repair (Infected)</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Time to repair (Disabled)</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Percentage of initially infected nodes</td>
<td>10%</td>
<td>10%</td>
<td>20%</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. 6 shows the time evolution of the percentage of nodes that are in each of the states defined in our model (and unless otherwise specified, each simulation plot is averaged over 15 runs). Simulation starts with 10% of nodes randomly infected. It is interesting that the curve corresponding to infected nodes provides a parallel behavior to the curve corresponding to disabled nodes, considering that in our model a node can only reach disabled state from infected state.
Fig. 6. Percentage of infected nodes during the first simulation, with a topology of 100 nodes.

Fig. 7. Ranking of nodes that have lost more connections during the first simulation with a topology of 100 nodes.

Fig. 8. Percentage of infected nodes during the second simulation, with a topology of 100 nodes.

Fig. 9. Percentage of infected nodes during the third simulation, with a topology of 200 nodes.

Fig. 10. Percentage of infected nodes during the fourth simulation, with a topology of 200 nodes.

Fig. 7 shows the number of affected connections per node. This information is useful in order to detect hot points in the network. These nodes could be protected (immunized) to avoid/minimize the impact of the epidemic.

Fig. 8 shows the time evolution of the percentage of nodes that are either infected or disabled during the simulation. In this case, the values chosen for $\beta$, $\delta$ and $c$ have led to the complete eradication of the infection of the network around $time = 75$.

Fig. 9 shows that once the network is infected at 20%, the percentage increases to values oscillating between 35% and 45%, while the value for disabled nodes keeps oscillating between 10% and 15%.

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

In this paper, a new model for the simulation of spreading of different failure types in GMPLS-based networks has been proposed. In order to define our model, a review of previous epidemic / failure propagation models has also been carried out. In this review we have pointed out different aspects related with transport networks that current models do not consider. To model how failures could affect current established paths, our model, called SID, includes node states defining partial failures (nodes are able to retain certain functionality) and link failures. These aspects have been taken into account in order to simulate the behavior of a GMPLS-based network.

In order to evaluate the performance of our model, intensive simulations have been carried out, including different network sizes and topologies. These simulations have reported three different scenarios: (a) the spreading of failures affects the whole network after a period of time, (b) the spreading of failures sharply decrease with a total recovery of the network and (c) the spreading of failures stabilizes affecting a specific percentage of the network. For each scenario, results allow us to identify critical zones of the network, in terms of number of infected nodes or number of affected connections.

As a future work, we plan to use this model in order to develop immunization techniques. These techniques could be used to minimize the impact of spreading of failures throughout the network. Our model could also be used as part of network robustness evaluation procedures in GMPLS-based networks.

References