Optical Switching and Networking 31 (2019) 1–7

Contents lists available at ScienceDirect

Optical Switching and Networking

journal homepage: www.elsevier.com/locate/osn

A study of the robustness of optical networks under massive failures

Jose L. Marzo [a,*], Sergio G. Cosgaya [a], Nina Skorin-Kapov [b], Caterina Scoglio [c], Heman Shakeri [c]

[a] Universitat de Girona, Institute of Informatics and Applications, Girona, Spain
[b] University Center of Defense, San Javier Air Force Base, MDE-UPCT, Santiago de la Ribera, Murcia, Spain
[c] Kansas State University, Department of Electrical and Computer Engineering, Manhattan, KS, USA

ARTICLE INFO

Keywords:
Network robustness
Network simulation
Epidemic models
Optical networks
Massive failures

ABSTRACT

In this paper, we provide a comparative analysis of network robustness for different synthetic and real optical network topologies under various types of massive failures using the Girona Network Robustness Simulator (GNRS). We model massive failures as random, targeted, and epidemic, the later of which has not yet been considered in the context of robustness. Results indicate that, in addition to the presence of hub nodes, which are critical for targeted attacks, the network diameter limiting the distance between hubs plays an important role in network robustness under epidemic massive failures.

1. Introduction

Massive failures caused by natural or man-made disasters in large-scale networks can affect considerable proportions of the world's inhabitants. In network-like infrastructures, the causes for such massive failures include: human errors, malicious attacks, large-scale disasters, and environmental challenges, among others [1–3]. Calculating the robustness of network infrastructures under such challenges can provide significant insight into the potential damage they can incur, as well as provide a foundation for creating more robust network topologies.

In this paper, we classify massive failures as random, targeted and epidemic and compare the robustness of various synthetic and real optical network topologies for each failure type, extending our previous work presented at the International Workshop on Resilient Networks Design and Modeling (RNDM 2017) [4]. The current paper describes the proposed epidemic model in detail, modified with respect to [4] by limiting the potential impact of failures (in terms of the number of hops). Furthermore, a new case study is provided applying the model to massive failures in optical networks presenting extensive new simulation results on synthetic and real optical telecommunication network topologies.

One of the main aims of research related to the robustness of graphs is to establish a unified measure quantifying network robustness. Establishing a single metric can facilitate network planning processes by allowing us to more easily compare different topologies, improve existing ones and design new networks which can perform well even in the presence of massive failures. Although significant research efforts have been underway in the field of network robustness, there is still no consolidated measure established which ties together all the previously proposed relevant metrics. In this work, we compute robustness based on a definition of R^* as a weighted sum of a set of the main metrics. The weights are computed based on the Principal Component Analysis allowing to draw the robustness surface as a heat map [5]. These calculations are integrated in a simulator called the Girona Network Robustness Simulator (GNRS) developed by the Broadband Communications and Distributed Systems group at the University of Girona. The GNRS computes a large set of metrics providing a heat map where the R^* values are plotted to provide a visual understanding of the robustness of a network in a massive failure scenario.

This paper is organized as follows. Section 2 provides preliminaries and previous work, introducing the robustness concept, massive failure models and their application to optical networks. The proposed epidemic model and computational mechanisms used to calculate the set of robustness metrics are described in Section 2. Section 4 presents the numerical results and Section 5 concludes the paper.

2. Preliminaries and related work

2.1. The robustness concept

In the context of networking, robustness can be defined as "the ability of a network to continue performing well even when it is subject to failures or attacks". Robustness computation in interconnected systems is

* Corresponding author.
E-mail addresses: joseluis.marzo@udg.edu (J.L. Marzo), s.gomez@udg.edu (S.G. Cosgaya), nina.skorinkapov@cud.upct.es (N. Skorin-Kapov), caterina@ksu.edu (C. Scoglio), heman@ksu.edu (H. Shakeri).

https://doi.org/10.1016/j.osn.2018.07.002
Received 18 April 2018; Received in revised form 12 July 2018; Accepted 25 July 2018
Available online 4 August 2018

measured using graph theory concepts, mainly centered on graph connectivity. Despite the robustness of graphs being extensively studied in the last decade, it still lacks a unifying framework embracing all the proposed metrics. An initial solution to compute the robustness (R) value was provided by Trajanovski et alt. in Ref. [6] as:

$$R = \sum_{k=1}^{n} s_k t_k$$

where s_k represents the weight and t_k the value of metric k. In the literature, there are two major issues related to this gap, a) how to select the most relevant metrics of a graph and b) how to weigh each of the n metrics to allow for their summation. In Ref. [5], a solution for the two aforementioned problems was proposed. The R^*-value and the concept of a robustness surface are introduced making use of the Principal Component Analysis (PCA) as:

$$R^* = \sum_{k=1}^{n} \hat{v}_k t_k$$

The process used to obtain the new n weights $\hat{v}_k$ in an automated way is described in Section 3.B.

2.2. Robustness metrics

In order to evaluate the robustness of a graph, several metrics can be applied as described in Refs. [6–9]. The can be grouped as structural, fragmentation-connectivity and centrality as follows.

1) Structural metrics

Structural metrics refer to classical graph parameters measuring the density (e.g. nodal degree) or the size (e.g. the diameter referring to the maximum distance between any arbitrary node pair).

2) Fragmentation & connectivity metrics

Fragmentation metrics address the number of components of a network and applicable only if the network is disconnected. Connectivity metrics measure how difficult it is to break the graph.

3) Centrality metrics

Centrality metrics measure the importance of individual elements in the graph based on their location. Common centrality metrics include: node and edge betweeness (i.e. the fraction of shortest paths that pass-through a given node/edge) or eigenvector centrality.

2.3. Modeling massive failures: random, targeted, and epidemic

The dynamics of massive failures can differ significantly depending on the type of failure considered. In this paper, we distinguish between three models of massive failures: random, targeted, and epidemic. Random failures represent component faults or unintentional and uncorrelated failures. Massive random failures present a theoretical reference since failures on a massive scale are almost always correlated. Targeted failures encompass human-driven attacks where the most important elements (e.g. hub nodes) are affected first, with the intentional goal of causing the most severe damage with minimum effort. Note, random and targeted failures typically are geographically spread out and do not propagate, but are limited to the nodes/links where the attacks or faults occur. Epidemic failures, on the other hand, refer to deliberate man-made attacks or natural disasters which cause cascading failures initiated at a single or multiple points of attack and spread via contagion phenomena. Such massive failures have not yet been considered in the context of robustness and is novel to this work.

Contagion phenomena appear in diverse natural and technological contexts, such as infectious disease spreading among humans, computer viruses propagating in computer networks and viral spreading of news in social networks. Mathematical and computational models of spreading processes have been developed to understand, predict, and control contagion phenomena, and to assess the associated risks. Classical models of contagion define nodal states (or compartments), such as susceptible, infected and infectious, and define rules for the transition from one state to another. An extensive survey concerning models for spreading processes in networks and control approaches is presented in Ref. [10]. Although pioneer works employ random network models [11], recent research efforts are aimed at studing spreading processes in general networks with no particular assumptions on the structure [12]. Epidemic models have been also proposed to represent specific types of cascading failures which propagate through neighbors in well-defined technological networks [13].

2.4. Massive failures in optical networks

Massive failures in optical networks can be gereated by large natural disasters or deliberate attacks caused by human intervention. Since the consequences of natural disasters can be the same as large-scale deliberate attacks in a specific geographical area, here we only discuss attack scenarios. Physical-layer attacks in optical networks are typically divided into two main categories according to the type of damage they incur: optical eavesdropping and service degradation (disruption) [14–16]. They can also be classified according to the attack method applied, distinguishing between signal insertion attacks, signal splitting attacks, and physical infrastructure attacks as described in Ref. [17].

Signal insertion attacks typically cause service degradation by injecting harmful signals into the network, such as high-power jamming signals which can cause increased crosstalk and nonlinear effects to co-propagating signals. In older networks comprised of Fixed Optical Add Drop Multiplexers (FOADMs) without power equalization capabilities, such attacks can be particularly harmful since the high-powered signal could propagate through the network causing system-wide damage. In networks equipped with Reconfigurable OADMs (ROADMs) and variable optical attenuators, signal insertion attacks typically will not propagate but can still cause significant damage to co-propagating signals at the link/node where the attack is initiated. Establishing and tearing down connections or sporadic jamming can also cause undesirable amplifier transients, where sharp changes in input power cause the power of the remaining channels to increase or decrease until the amplifier settles in the steady-state. Such oscillations are short-lived but may propagate causing transients on successive links. Signal splitting attacks refer to attacks removing (splitting) part of a legitimate signal, either for eavesdropping or signal degradation purposes. Physical infrastructure attacks encompass all attacks which tamper with the physical optical components, such as cutting a fiber, damaging components, or unplugging connections. They can be individual component attacks mimicking single link or node failures, disaster-like attacks incurring multiple failures in a specific geographical area, or critical location attacks aimed at specifically attacking weak point or hubs in the optical network. Examples of critical location attacks can include targeting subsea landing points, specific data center locations, or SDN-controller locations in future SDN networks.

In the context of massive failures, the aforementioned physical-layer optical network attacks can be grouped as follows. Random massive failures, corresponding to a set of uncorrelated single failures, can correspond to a set of any of the described non-propagating optical network attacks, such as several single component physical infrastructure attacks. Targeted massive failures can be used to model critical location attacks, as well as multiple non-propagating signal insertions attacks (such as high-power jamming in a ROADM-based network), or multiple eavesdropping attacks at targeted locations. Epidemic massive failures can represent propagating signal insertion attacks, such as in-band jamming in FOADM-based networks. An example of such an attack is