Epidemic and Cascading Survivability of Complex Networks

M. Manzano, E. Calle, J. Ripoll, A.Manolova Fagertun,
V. Torres-Padrosa, S. Pahwa, C. Scoglio

Abstract—Our society nowadays is governed by complex networks, examples being the power grids, telecommunication networks, biological networks, and social networks. It has become of paramount importance to understand and characterize the dynamic events (e.g. failures) that might happen in these complex networks. For this reason, in this paper, we propose two measures to evaluate the vulnerability of complex networks in two different dynamic multiple failure scenarios: epidemic-like and cascading failures. Firstly, we present *epidemic survivability* (ES), a new network measure that describes the vulnerability of each node of a network under a specific epidemic intensity. Secondly, we propose *cascading survivability* (CS), which characterizes how potentially injurious a node is according to a cascading failure scenario. Then, we show that by using the distribution of values obtained from ES and CS it is possible to describe the vulnerability of a given network. We consider a set of 17 different complex networks to illustrate the suitability of our proposals. Lastly, results reveal that distinct types of complex networks might react differently under the same multiple failure scenario.

Index Terms—Network Characterization, Epidemics, Cascading Failures, Multiple Failures, Complex Networks

I. INTRODUCTION

Many different protection and restoration techniques for single failures have been extensively analyzed in recent decades (e.g. see [1]). Furthermore, multiple failures such as natural disasters or physical attacks have also been studied [2]. According to the taxonomy introduced in [3], there are two types of multiple failures. While *static* multiple failures are essentially one-off failures that affect one or more elements (nodes or links) simultaneously at any given point, *dynamic* failures have a temporal dimension. In this paper we consider *dynamic* multiple failures, which we implement through *epidemic* and *cascading* failures. On one hand, an epidemic-like failure propagation occurs when, at a given time, a node or a group of them start spreading an infection. In this case the failure (e.g. infection) propagates through physical neighbors. On the other hand, cascading failures occur when a node (or a group of them) fails, and as a consequence, other parts in the network fail as well due to an overloading of the capacity. Cascading failures do not necessarily propagate through physical contact, i.e. one node failure can cause a failure to a non-adjacent node due to the network load balancing.

Marc Manzano, Eusebi Calle, Jordi Ripoll and Victor Torres-Padrosa are with University of Girona, Spain. Anna Manolova Fagertun is with Technical University of Denmark, Denmark. Sakshi Pahwa and Caterina Scoglio is with Kansas State University, USA. Corresponding author: Marc Manzano (email: mmanzano@eia.udg.edu - marcmanzano@ksu.edu).

In contrast with single failures, in the case of multiple failures it is nonviable to define proper reactive strategies. Thus, since the reasonable approach to address such large-scale failures involves the designing phase of a network, it has become of paramount importance to define new metrics able to evaluate the vulnerability of networks in the case of multiple failure scenarios. Appropriate metrics can help network engineers and operators to detect the most critical parts of a network. Although a new generic metric suitable to accurately evaluate the robustness in static multiple failure scenarios has been recently presented in [3], to the best of our knowledge there are no metrics able to evaluate the robustness under dynamic multiple failure scenarios.

In our previous work [4] we presented a metric called epidemic survivability. In this paper we go one step further and we extend the work by considering broader type of failures: dynamic multiple failures. In addition, we extend the number of networks considered for testing of the failure scenarios to 17, as compared to 6 in the previous work. Consequently, here we consider 2 telecommunication networks, 2 Internet Autonomous Systems (AS) networks, 5 synthetic generated networks, 1 biological network, 3 social networks and 4 power grid networks. Our aim is to take into account a wide range of different types of complex networks, and evaluate them under dynamic multiple failure scenarios. Within this context, the main contributions of this paper are:

1) a new network measure called *epidemic survivability* (ES). This feature describes the vulnerability of each node of a network under a specific epidemic scenario.
2) a new network measure called *cascading survivability* (CS), which characterizes how potentially injurious a node is according to a specific cascading failure scenario.

We believe that our proposals can be used by the network research community to evaluate the criticality of nodes of a network under failure propagation scenarios. In addition, our metrics can be used to amplify general recovery metrics such as [5].

II. NETWORK TOPOLOGIES

In this section we present the set of seventeen network topologies considered in our work. These networks have been chosen in order to represent a wide variety of complex network topology types:

1) *abilene93*: a small network that has been chosen because of its underlying AS topology structure.

2) *cogentco197*: a real telecommunications network that has been taken from the repository provided in [6].
3) *er400*: a random network that has been generated using the Erdős-Rényi model [7].
4) *powerlaw400*: a power-law network that has been generated using the Barabási-Albert (BA, preferential attachment mechanism) model [8].
5) *homoge400*: a homogeneous network (a network where all the nodes have equal node degree) that has been generated, being a toroidally-periodic rectangular lattice of size 20×20. Although this network is not a complex network, it has been considered for comparison purposes.
6) *bt400*: this topology has been obtained by manipulating a previously generated topology using BRITE.
7) *bo1458*: a protein interaction network for yeast [9].
8) *col4158*: a collaboration network of Arxiv's *General Relativity* category [10].
9) *col8638*: a collaboration network of Arxiv's *High Energy Physics Theory* category [10].
10) *cost37*: a Pan-european communications reference network.
11) *europg1494*: an approximated model of the european power grid network [11].
12) *fb4039*: this network represents *circles* or *friends list* of the popular social network Facebook [12].
13) *wspg4941*: a topology of the Western States Power Grid of the United States [13].
14) *pgieee118* and *pgieee300*: these two topologies are reference IEEE power grid networks [14].
15) *AS25357*: an AS network from 2012 [15].
16) *AS26475*: this network is the largest CAIDA AS connected graph from the network set available in November 2007 [10].

The *col4158*, *col8638*, *fb4039* and *AS26475* networks have been obtained from the SNAP dataset [16]. All of the networks are connected and considered as symmetric graphs. It is worth noting that some of the networks were not connected, and a post-processing has been done in order to obtain the largest connected component. Table I shows the networks that have been post-processed because they were disconnected. Furthermore, Table II and Table III present several characteristics of this set of networks, some of which are presented with their *standard deviation*. As it can be observed, we have considered a heterogeneous set of networks with respect to the number of nodes, ranging from 37 to 26475.

The *fb4039* network shows the highest average nodal degree ($\langle k \rangle = 43.69$), what means that every person has an average of about 44 friends in this social network. The two AS networks (*AS25357* and *AS26475*) present the highest mean degree of first neighbors ($\langle d \rangle$) and maximum degree (k_{max}), i.e. in *AS25357* there is an AS that is connected to other (k_{max}) 3781 ASes, and some of them have a high node degree as well. A high k_{max} is an indicator of vulnerability, depicting that removal of such a node could seriously damage the network. Networks with high values of the largest eigenvalue

of the adjacency matrix (or spectral radius, λ_1) and algebraic connectivity (μ_{N-1}) are more robust. In this case, the *fb4039* network shows the highest spectral radius and the *er400* presents the highest algebraic connectivity. For this reason, these two networks are supposed to be most robust than the rest of them in the case of failures.

Regarding the average shortest-path length ($\langle l \rangle$) it is shown that two power grid networks (*europg1494* and *wspg4941*) have the higher values and consequently are more vulnerable. This is due to the fact that, traditionally, power grid networks have a tree-like structure. Furthermore, the average node betweenness centrality ($\langle b \rangle$) of *cost37*, *cogentco197* and *abilene93* shows that these three topologies have an excess of centrality measures for some nodes, indicating the vulnerability of networks under targeted failures. The absence of 3-cycles in the clustering coefficient ($\langle C \rangle$) measurements reveal that the *homoge400* and *cost37* lack two-hop paths to re-route the traffic in case of failure of one of its neighbors. Finally, networks with negative values of assortativity (r) have an excess of radial links, i.e., links connecting nodes of dissimilar degrees. Such a property is typical of technological networks [17].

This initial network analysis of the considered set of topologies reveals that none of the networks can be considered as the most robust for all of the metrics. Besides, the vulnerability of the networks is going to differ depending on the considered type of multiple failures. As a consequence, it is necessary to define new metrics able to characterize how robust a network is in a specific scenario. The following two sections present two new measures to evaluate network vulnerability in the case of epidemic-like and cascading failures.

III. EPIDEMIC-LIKE FAILURES

Epidemic models are used to model the spreading of events (e.g. failures) in several types of complex networks. These models have been used in a wide variety of research fields. In this section we review the classical epidemic models and introduce a novel network measure that is suitable for evaluating the vulnerability under epidemic-like failure scenarios.

A. Epidemic Models

Epidemic dynamics in complex networks have undergone extensive research [18], [19] [20], [21]. As a consequence, many epidemic models have been proposed and several families are described in the literature (see Chapter 8 in [22], Chapter 17 in [23] and Chapter 14 in [24]). 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 ($S \rightarrow I$). 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 probability of becoming susceptible again. Therefore, individuals will change their state from susceptible to infected, and vice versa, several times ($S \leftrightarrows I$).

TABLE I

NETWORKS THAT WERE DISCONNECTED AND FOR WHICH A POST-PROCESSING HAS BEEN DONE TO OBTAIN THE LARGEST CONNECTED COMPONENT.

Topology	List of $|N| \times$ number of components
bo1458	1458×1; 7×4; 6×3; 5×5; 4×10; 3×25; 2×101; 1×24
col4158	4158×1; 14×1; 12×1; 10×1; 9×2; 8×6;
	7×8; 6×12; 5×17; 4×30; 3×98; 2×177; 1×1
col8638	8638×1; 21×1; 11×1; 9×2; 8×6; 7×11;
	6×8; 5×21; 4×45; 3×67; 2×264; 1×2
europg1494	1494×1; 1×19
AS25357	25357×1; 2×5

TABLE II

MAIN NETWORK FEATURES. THE TABLE DISPLAYS, FROM LEFT TO RIGHT: TOPOLOGY NAME, NUMBER OF NODES, AVERAGE NODAL DEGREE $\pm$ *standard deviation* (STDEV), MEAN DEGREE OF FIRST NEIGHBORS $\pm$ STDEV, LARGEST EIGENVALUE OF THE ADJACENCY MATRIX, MAXIMUM DEGREE $k_{\max}$ AND THE SECOND SMALLEST EIGENVALUE OF THE LAPLACIAN MATRIX (THE SO-CALLED *algebraic connectivity*).

Topology	N	$\langle k \rangle \pm$ StDev	$\langle d \rangle \pm$ StDev	λ_1	$k_{\max}$	μ_{N-1}
abilene93	93	2.88 $\pm$2.71	6.76 $\pm$2.76	5.016	12	0.07607
cogentco197	197	2.46 $\pm$1.05	2.91 $\pm$0.92	3.778	9	0.00858
er400	400	7.81 $\pm$2.80	8.89 $\pm$1.01	8.848	15	0.90416
powerlaw400	400	2.00 $\pm$3.25	9.47 $\pm$11.81	7.013	47	0.00463
homoge400	400	4.00 $\pm$0.00	4.00 $\pm$0.00	4.000	4	0.09788
bt400	400	3.74 $\pm$2.17	5.44 $\pm$1.61	5.195	11	0.01013
bo1458	1458	2.67 $\pm$3.45	9.65 $\pm$10.74	7.535	56	0.02126
col4158	4158	6.45 $\pm$8.62	11.60 $\pm$9.02	45.616	81	0.03530
col8638	8638	5.74 $\pm$6.45	11.25 $\pm$6.65	31.034	65	0.02441
cost37	37	3.08 $\pm$0.85	3.31 $\pm$0.45	3.399	5	0.15857
europg1494	1494	2.88 $\pm$1.75	4.17 $\pm$1.58	5.027	13	0.00170
fb4039	4039	43.69 $\pm$52.41	105.55 $\pm$91.30	162.373	1045	0.01812
wspg4941	4941	2.66 $\pm$1.79	3.96 $\pm$1.93	7.483	19	0.00076
pgieee118	118	3.03 $\pm$1.56	3.95 $\pm$1.13	4.105	9	0.02714
pgieee300	300	2.72 $\pm$1.54	3.86 $\pm$1.71	4.126	11	0.00938
AS25357	25357	5.91 $\pm$48.03	659.73 $\pm$827.98	103.361	3781	0.10768
AS26475	26475	4.03 $\pm$33.37	471.27 $\pm$644.72	69.642	2628	0.02043

TABLE III

NETWORK FEATURES. THE TABLE DISPLAYS, FROM LEFT TO RIGHT: TOPOLOGY NAME, AVERAGE SHORTEST PATH LENGTH $\pm$ STDEV, NORMALIZED AVERAGE BETWEENNESS CENTRALITY $\pm$ STDEV, AVERAGE CLUSTERING COEFFICIENT $\pm$ STDEV, AND ASSORTATIVITY COEFFICIENT $|r| \leq 1$.

Topology	$\langle l \rangle \pm$ StDev	$\langle b \rangle \pm$ StDev	$\langle C \rangle \pm$ StDev	r
abilene93	3.92 $\pm$1.32	0.0529 $\pm$0.0551	0.51 $\pm$0.48	-0.5130
cogentco197	10.52 $\pm$5.09	0.0585 $\pm$0.0665	0.12 $\pm$0.32	$+0.01956$
er400	3.13 $\pm$0.73	0.0103 $\pm$0.0037	0.02 $\pm$0.07	-0.07229
powerlaw400	6.01 $\pm$2.16	0.0175 $\pm$0.0594	0.64 $\pm$0.47	-0.16512
homoge400	10.03 $\pm$4.10	0.0276 $\pm$0.0000	0.00 $\pm$0.00	$+1.0000$
bt400	10.12 $\pm$4.21	0.0202 $\pm$0.0357	0.16 $\pm$0.27	-0.29646
bo1458	6.81 $\pm$2.04	0.0039 $\pm$0.0110	0.56 $\pm$0.47	-0.20954
col4158	6.04 $\pm$1.57	0.0012 $\pm$0.0034	0.71 $\pm$0.35	$+0.63919$
col8638	5.94 $\pm$1.50	0.0005 $\pm$0.0015	0.65 $\pm$0.37	$+0.23892$
cost37	4.05 $\pm$1.90	0.0782 $\pm$0.0756	0.00 $\pm$0.00	-0.01510
europg1494	18.88 $\pm$8.73	0.0119 $\pm$0.0304	0.27 $\pm$0.40	-0.11965
fb4039	3.69 $\pm$1.19	0.0006 $\pm$0.0116	0.62 $\pm$0.20	$+0.06358$
wspg4941	18.98 $\pm$6.50	0.0036 $\pm$0.0160	0.32 $\pm$0.44	$+0.00346$
pgieee118	6.30 $\pm$2.81	0.0457 $\pm$0.0723	0.22 $\pm$0.36	-0.15257
pgieee300	9.93 $\pm$4.06	0.0299 $\pm$0.0546	0.31 $\pm$0.42	-0.22063
AS25357	3.39 $\pm$0.70	0.0001 $\pm$0.0020	0.73 $\pm$0.36	-0.18540
AS26475	3.87 $\pm$0.90	0.0001 $\pm$0.0020	0.58 $\pm$0.46	-0.19465

The *Susceptible-Exposed-Infected-Susceptible* (SEIS) model is based on the SIS model, and takes into consideration the exposed or latent period of the disease ($S \rightarrow E \rightarrow I \rightarrow S$). The third broad family is *Susceptible-Infected-Removed* (SIR), which extends the SI model to take into account a removed state. In the SIR model, an individual can be infected just once because when the infected individual recovers, becomes either immune or dead, and will no longer pass the infection onto others ($S \rightarrow I \rightarrow R$). 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 ($S \rightarrow I \rightarrow D \rightarrow R$). The second one considers that after an individual becomes removed, it remains in that state for a specific period of time and then goes back to the susceptible state ($S \rightarrow I \rightarrow R \rightarrow S$).

Regarding communication networks, an extension of the SIS model, which is called Susceptible-Infected-Disabled-Susceptible (SIDS), was proposed in [25] in order to overcome the limitations of the SIS model with respect to optical transport networks. The SIDS model (*Susceptible$\leftrightarrows$Infected$\rightarrow$Disabled$\rightarrow$Susceptible*) is proposed as one of the first models to consider real telecommunication networks features and it relates each state to a functionality of the network devices. In addition, other epidemic models have also been proposed for wireless telecommunication networks [26].

In this paper we propose a new network measure taking into account the SIS model, which is characterized by two probabilities: (a) β, the probability of being infected by an already infected node; and (b) δ, the probability of an infected node to recover and become susceptible again. However, our proposal can be also applied to any other epidemic model and we plan to do so in the future.

Furthermore, according to [21] and from the following equation:

$$s = \frac{\beta}{\delta} \lambda_1 \qquad (1)$$

where s is the *epidemic intensity* and λ_1 is the network's largest eigenvalue of the adjacency matrix, which has been typically used to predict network robustness, when $s > 1$ an epidemic survives and the spread of the infection might never die. Thus, in order to obtain comparable results between networks with respect to our proposal (*epidemic survivability*), s must be a parameter of our new measure.

In this work we have fixed $s = 3$ for all networks, in order to obtain comparable results, and we have obtained a specific β value for each network from the equation $\beta = \frac{s\delta}{\lambda}$.

B. Epidemic Survivability

Here we present our new network measure called *epidemic survivability* (ES). We define our proposal as the probability for each node of a given network to be eventually infected

(i.e., in a large enough amount of time steps), given a specific *epidemic intensity* (s). This probability of each node asymptotically reaches a stationary state, according to simulations and theoretical models. *Epidemic survivability* can be described as the proportion of time for which each node of a given network has been infected for a given s, in a large enough period of time, as shown in Eq. 2:

$$ES_i(s) = \frac{\text{time for which node } i \text{ has been infected}}{\text{total time}} \qquad i = 1, \ldots, N \quad (2)$$

where N is the number of nodes of the network. As a result, ES has a value between 0 and 1 for each node, where higher the value, more vulnerable is the node under the specified epidemic scenario. Formally, from the SIS model, *epidemic survivability* can be computed with the following equation:

$$ES_i^* = \frac{1}{1 + (\frac{\beta}{\delta} \sum_{j \sim i} ES_j^*)^{-1}} \qquad i = 1, \ldots, N \quad (3)$$

where $*$ means *at the stationary state* and $j \sim i$ is the set of *neighbors* of node i. Here, it is assumed that δ and s are given as parameters and β is obtained from the equation $\beta = \frac{s\delta}{\lambda_1}$. Thus, it can be observed that Eq. 3 is a recursive formula and must be initialized with a value. We define this initialization of the probabilities in Eq. 4:

$$ES_{i,\text{approx}}^* = (1 - \frac{1}{s}) \qquad i = 1, \ldots, N \quad (4)$$

which corresponds to the solution of Eq. 3 for the case of a homogeneous/regular network. Moreover, a procedure for computing *epidemic survivability* is provided in Algorithm 1. As it can be observed, the method requires five parameters: the network $\mathcal{G}$ and four constants (s, δ, k and tol). The first two steps (lines 3 and 4) compute the largest eigenvalue of the given network and thus obtain the β value of the epidemic model. Then, all probabilities are initialized as stated in Eq. 4 (lines 5 to 7). Therefore, in the main loop of line 8 the new probability of each node is computed as defined in Eq. 3 (lines 9 to 11). After that, the absolute error is checked (lines 12 to 14) and if it results lower than the given tolerance (tol) then the algorithm ends, and returns the array containing the *epidemic survivability* of each node of the network. If the absolute error is still higher than tol another iteration is performed.

C. The distribution

When computing the *epidemic survivability* for the nodes of a network, according to a specified set of parameters, it is interesting to analyze the distribution of ES values. If these values are sorted, for example, in descending order, it facilitates the comparison between network topologies when considering the same failure propagation scenario for all of them. This approach is illustrated in Fig. 1 which displays the *epidemic survivability* distribution, the ES of each node, for the 17 networks in a specific epidemic scenario. As can be observed, the two AS networks (*AS25357* and *AS26475*) together with the two collaboration networks (*col4158* and

Algorithm 1 Compute *epidemic survivability*.

Require: $s \geq 1, d > 0, k > 0, tol > 0, connected \; \mathcal{G}$
1: **Input:** a graph $\mathcal{G}$ and the constants s (epidemic intensity), δ (repairing rate), k (maximum number of iterations) and tol (tolerance).
2: **Output:** an array containing the *epidemic survivability* of each node.
3: $\lambda \leftarrow$ spectralRadius($\mathcal{G}$) {largest eigenvalue}
4: $\beta \leftarrow \frac{s*\delta}{\lambda}$
5: **for all** $v \in vertexSet(\mathcal{G})$ **do**
6: $\quad P_{ES}[v] = (1 - \frac{1}{s})$
7: **end for**
8: **for** $c = 1 \rightarrow k$ **do**
9: $\quad$ **for all** $v \in vertexSet(\mathcal{G})$ **do**
10: $\quad\quad P_{aux}[v] = \frac{1}{1+(\frac{\beta}{\delta} \sum_{j \sim v} P_{ES}[j])^{-1}}$
11: $\quad$ **end for**
12: $\quad$ **if** $(\|P_{aux} - P_{ES}\|) < tol$ **then**
13: $\quad\quad$ break
14: $\quad$ **end if**
15: $\quad P_{ES} \leftarrow P_{aux}$
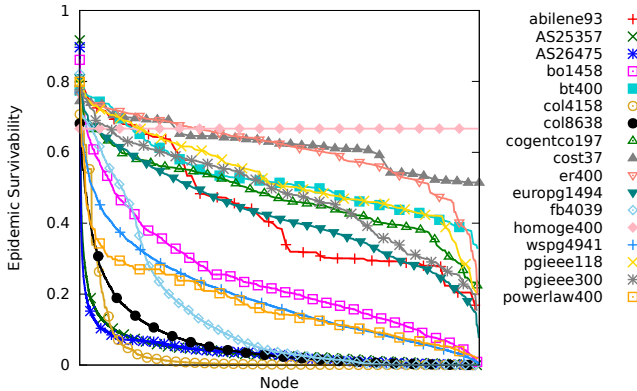16: **end for**
17: **return** P_{ES}

Fig. 1. *Epidemic survivability* distribution, sorted from major to minor values, of all networks. In this case the set of parameters has been: $s = 3$, $\delta = 0.3$, $k = 2000$ and $tol = 1e^{-8}$. The X-axis shows the nodes of the network, their index not showed for the sake of clarity.

col8638) show the lowest ES distributions, demonstrating that such networks are more robust than the rest of networks, in the case of an epidemic-like failure with epidemic intensity $s = 3$.

It is worth noting that different types of complex networks show different ES distribution curves. While AS and collaboration networks show power-law-like curves, power grids, telecommunication networks, synthetic networks and the biological network depict more smooth-decreasing curves. On one hand, curves showing a rapid decrease (i.e. power-law-like profile) would be expected in complex networks regarding critical infrastructures. This is due to the fact that only a small portion of the nodes of the network would be highly vulnerable, and consequently, it would require less effort (e.g. economical) from the network engineer or operator to protect it. On the other hand, regarding social networks one could expect different curve profiles, depending on the purpose of the social network (e.g. a country's government interested

in controlling its social networks would prefer flatter curves, because there would not be any node with a high spreading potential).

IV. CASCADING FAILURES

Cascading failure models have been used to understand dynamic multiple failures in different types of complex networks. In this section we provide an overview about the main cascading failure models that have been used in the literature. Moreover, we present a new network measure to evaluate the vulnerability of complex networks under these types of failures.

A. Cascading Failure Models

Cascading failures have been extensively studied in the literature. Some of the most well-known models are presented next. In [27] one of the first cascading failure models was presented, which focused on random complex networks. Contemporarily, the authors of [28] presented a simple but functional model. Later on, the model was enhanced in [29] by keeping an auxiliary cost matrix related with the efficiency metric [30], [31]. Furthermore, in [32] the authors proposed an analytically tractable loading-dependent cascading failure model. In [33] an AC blackout model representing most of the interactions observed in cascading failures was presented. Recently, in [34] a cascading failure model for inter-domain routing systems was presented. Moreover, the authors proposed two metrics to assess the impact of a cascading failure: the proportion of failure nodes and the proportion of failed links.

As previously stated in this work, our objective is to define a metric able to characterize the vulnerability of the elements of a network (i.e. in this case nodes) under cascading failures. To do so, we have chosen the model presented in [28]. According to this model, each node j is related with a load L_j. The load at each node is the node betweenness centrality, i.e. the number of shortest paths passing through the node. Then, the capacity can be defined as a proportional value to the initial load L_j, as denoted by Eq. 5:

$$C_j = (1 + \alpha) \cdot L_j \qquad j = 1, 2, \ldots, N \qquad (5)$$

where N is the number of nodes of the network and α, the *tolerance* parameter of the model, is a constant that must be $\alpha \geq 0$. This parameter is related with the concept of *capacity dimensioning* of a network, which is of paramount importance at the designing phase of a network (e.g. a critical infrastructure such as a power grid). An appropriate level of *over-dimensioning* can prevent a network from cascading failures. However, a higher α typically involves a higher economical budget. Therefore, network engineers must seek a trade-off between these two factors.

As defined by the model in [28], we focus on cascades triggered by the removal of a single node. This event, in general, causes changes in the distribution of shortest paths. As a result, after an initial node failure, the new load of the

nodes (L'_j) might be different from the initial load (L_j). Then, for each node, if the expression of Eq. 6 is satisfied:

$$L'_j > C_j \qquad (6)$$

the node j overloads and fails, which might cause subsequent overloading failures on the rest of nodes of the network.

Finally, we note that in the results presented further in this section we have assumed an $\alpha = 0.05$ for all networks, with the purpose of allowing comparison among them.

B. Cascading Survivability

Our new network measure called *cascading survivability* (CS) is presented below. *Cascading survivability* evaluates how potentially injurious a node is according to a specific cascading failure scenario. In other words, CS can be described as shown in Eq. 7:

$$CS_i(\alpha) = \frac{\text{nodes that fail if node } i \text{ initially fails}}{\text{all nodes in the network} - 1} \quad 1 = 1, \ldots, N \quad (7)$$

where N is the number of nodes of the network. As observed, α is a parameter of CS, what means that for different α distinct CS values might be obtained. *Cascading survivability* takes values in the range between 0 and 1 for each node, where higher the value, more harmful is the node under a specific cascading failure scenario.

Algorithm 2 Compute *cascading survivability*.

Require: $\alpha \geq 0, connected\ \mathcal{G}$
1: **Input:** a graph $\mathcal{G}$ and the constant α (tolerance parameter).
2: **Output:** an array containing the *cascading survivability* of each node.
3: $N \leftarrow$ vertexSize($\mathcal{G}$))
   {initializing load and capacity of each node}
4: **for all** $v \in vertexSet(\mathcal{G})$ **do**
5:      $L[v] =$ NodeBetweennessCentrality($\mathcal{G}$)
6:      $C[v] = (1 + \alpha) \cdot L[v]$
7: **end for**
8: **for all** $v \in vertexSet(\mathcal{G})$ **do**
9:      $F \leftarrow$ add(v) {add node v to the list of nodes that are going to fail}
10:      **while** F is not empty **do**
11:          $\mathcal{G}' \leftarrow$ removeNodes($\mathcal{G}$,F) {removes from $\mathcal{G}$ all nodes in F. After the operation F is empty.}
12:          **for all** $u \in vertexSet(\mathcal{G}')$ **do**
13:              $L'[u] =$ NodeBetweennessCentrality($\mathcal{G}'$)
14:              **if** $L'[u] > C[u]$ **then**
15:                  $F \leftarrow$ add(u)
16:                  $CS[v] = CS[v] + 1$ {increase in 1 the number of nodes that have failed due to the initial failure of v}
17:              **end if**
18:          **end for**
19:      **end while**
20: **end for**
21: **for all** $v \in vertexSet(\mathcal{G})$ **do**
22:      $CS[v] = \frac{CS[v]}{N-1}$
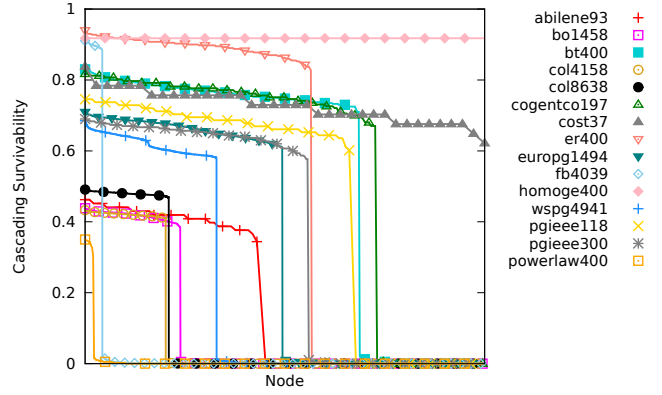23: **end for**
24: **return** CS

Fig. 2. *Cascading survivability* distribution, sorted from major to minor values, of all networks. In this case we have considered $alpha = 0.05$. The X-axis shows the nodes of the network, their index not showed for the sake of clarity.

We have defined a procedure to compute the *cascading survivability* of the nodes of a network, which is presented in Algorithm 2. As shown, the method requires two parameters: the network $\mathcal{G}$ and the tolerance parameter α. First of all, the initial load and capacity of each node is computed (lines 4 to 7). Then, an initial failure is caused, for each one of the nodes of the given network, one at a time (lines 8 to 20). For each initial failure (line 9) and as well as at each step of the spreading of the cascade, (lines 10 to 19), the new load of the remaining nodes of the network is computed (line 13). If the new load becomes higher than the capacity at any step, then the *cascading survivability* of the node that initially triggered the failure is increased (lines 14 to 17). Finally, the CS of each node is normalized (lines 21 to 23).

C. The distribution

When computing the *cascading survivability* for the nodes of a network, given a network and a specific α, it is worth noting the utility of analysing the distribution of the CS values, as previously illustrated for *epidemic survivability* in Section III-C.

By sorting the CS values in descending order it is possible to compare different networks, according to a specific cascading failure scenario denoted by α. Fig. 2 shows the CS distribution of 15 of the networks considered in this work, in the case of a cascading failure with $\alpha = 0.05$. It is interesting to note that most of the networks show a bimodal CS distribution. This means that the nodes of such networks can be clearly divided in two groups: *harmful* and *not significant* in the case of a cascading failure. This behavior has been observed in other works such as [35]. Moreover, as observed, depending on the network the percentage of harmful nodes might vary. For instance, the *fb4039* and the *er400* networks start the distribution around 0.9, however it is in the former where only a 5% of the nodes represents a *threat* in the case of cascading failures, while in the latter it is about 55%. Finally, different types of complex networks show different CS distribution curves, just like they show different ES curves as represented in Section III-C.

V. SUMMARY AND CONCLUSIONS

In this paper we have proposed two new measures to evaluate the vulnerability of complex networks in two different dynamic multiple failure scenarios: epidemic-like and cascading failures.

Firstly, we have proposed a new network measure called *epidemic survivability* (ES), which describes the vulnerability of each node of a network under a specific epidemic-like failure propagation scenario. Besides, a procedure to compute our novel measure has been provided. Sorting the ES distribution of values of all nodes of a network in descending order, it is possible to analyze which nodes would be more vulnerable in the case of an epidemic failure. Furthermore, using this ES distribution, network vulnerability can be compared for a specific epidemic scenario.

Secondly, we have presented a new network measure called *cascading survivability* (CS), which characterizes how potentially dangerous a node is according to a specific cascading failure scenario. In addition, we have provided a procedure to compute CS. Then, as for the *epidemic survivability* metric, we have noted the inherent usability related to the CS distribution.

Lastly, we have computed ES and CS for the set of networks considered in this work, being each measure dependent on a specific failure scenario. Results have shown that distinct types of complex networks might react differently under the same dynamic multiple failure. In addition, results have revealed that a complex network might be more or less vulnerable, depending on the specific type of multiple failure scenario (i.e. epidemic-like or cascading failures). For instance, while the *cogentco197* network shows a smooth decreasing curve of ES, the same network shows a bimodal distribution of CS, where about 25% of nodes are not dangerous in the case of cascading failures.

REFERENCES

[1] J. P. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," *Computer Networks*, vol. 54, no. 8, pp. 1245–1265, 2010.

[2] M. Azim and A. El-semary, "Vulnerability assessment for mission critical networks against region failures: A case study," in *Proceedings of the 2nd International Conference on Communications and Information Technology (ICCIT)*, 2012.

[3] M. Manzano, E. Calle, V. Torres-Padrosa, J. Segovia, and D. Harle, "Endurance: A new robustness measure for complex networks under multiple failure scenarios," *Computer Networks*, no. 0, pp. –, 2013, in Press.

[4] M. Manzano, E. Calle, J. Ripoll, A. Fagertun, and V. Torres-Padrosa, "Epidemic survivability: Characterizing networks under epidemic-like failure propagation scenarios," in *Proceedings of the 9th International Conference on the Design of Reliable Communication Networks (DRCN)*, 2013, pp. 95–102.

[5] P. Cholda, A. Jajszczyk, and K. Wajda, "A unified quality of recovery (QoR) measure," *International Journal of Communication Systems*, vol. 21, no. 5, pp. 525–548, 2008.

[6] www.topology-zoo.org, [Online; accessed 28-Sep-2013].

[7] B. Bollobás, "Random graphs," *Cambridge University Press*, vol. 73, 2001.

[8] A. L. Barabasi and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, 1999.

[9] H. Jeong, S. Mason, A. Barabasi, and Z. Oltvai, "Lethality and centrality in protein networks," *Nature*, vol. 411, pp. 41–42, 2001.

[10] J. Leskovec, J. Kleinberg, and C. Faloutsos, "Graph evolution: Densification and shrinking diameters," *ACM Transactions on Knowledge Discovery from Data*, vol. 1, no. 1, p. 2, 2007.

[11] N. Hutcheon and J. W. Bialek, "Updated and validated power flow model of the main continental european transmission network," in *Proceedings of the IEEE PowerTech 2013*, 2013.

[12] J. J. McAuley and J. Leskovec, "Learning to discover social circles in ego networks." in *NIPS*, 2012, pp. 548–556.

[13] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.

[14] University of Washington, http://www.ee.washington.edu/research/pstca/, [Online; accessed 28-Sep-2013].

[15] The DIMES project, http://www.netdimes.org/, [Online; accessed 28-Sep-2013].

[16] Stanford Network Analysis Project, http://snap.stanford.edu/, [Online; accessed 28-Sep-2013].

[17] M. E. J. Newman, "The structure and function of complex networks," *SIAM Review*, vol. 45, pp. 167–256, 2003.

[18] R. Pastor-Satorras and A. Vespignani, "Epidemic spreading in scale-free networks," *Physical Review Letters*, vol. 86, no. 14, pp. 3200–3203, 2001.

[19] M. E. J. Newman, "Spread of epidemic disease on networks," *Physical Review E*, vol. 66, p. 016128, 2002.

[20] R. Pastor-Satorras and A. Vespignani, "Epidemic dynamics in finite size scale-free networks," *Physical Review E*, vol. 65, p. 035108, 2002.

[21] D. Chakrabarti, Y. Wang, C. Wang, J. Leskovec, and C. Faloutsos, "Epidemic thresholds in real networks," *ACM Transactions on Information and System Security*, vol. 10, no. 4, pp. 1–26, 2008.

[22] T. Lewis, *Network Science: Theory and Applications.* Wiley, 2009.

[23] M. E. J. Newman, *Networks: An Introduction.* Oxford University Press, 2010.

[24] R. Cohen and S. Havlin, *Complex Networks: Structure, Robustness and Function.* Cambridge University Press, 2010.

[25] E. Calle, J. Ripoll, J. Segovia, P. Vila, and M. Manzano, "A multiple failure propagation model in GMPLS-based networks," *IEEE Network*, vol. 24, no. 6, pp. 17–22, 2010.

[26] Y. M. Ko and N. Gautam, "Epidemic-based information dissemination in wireless mobile sensor networks." *IEEE/ACM Transactions on Networking*, vol. 18, no. 6, pp. 1738–1751, 2010.

[27] D. J. Watts, "A simple model of global cascades on random networks," *Proceedings of the National Academy of Sciences*, vol. 99, no. 9, pp. 5766–5771, 2002.

[28] A. E. Motter and Y. C. Lai, "Cascade-based attacks on complex networks," *Physical Review E*, vol. 66, no. 6, pp. 065 102+, 2002.

[29] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Physical Review E*, vol. 69, p. 045104, 2004.

[30] V. Latora and M. Marchiori, "Efficient behavior of small-world networks," *Physical Review Letters*, vol. 87, no. 19, p. 198701, 2001.

[31] Y.-C. Lai, A. Motter, and T. Nishikawa, "Attacks and cascades in complex networks,," *Lecture Notes in Physics*, vol. 650, pp. 299–310, 2004.

[32] I. Dobson, B. A. Carreras, and D. E. Newman, "A loading-dependent model of probabilistic cascading failure," *Probability in the Engineering and Informational Sciences*, vol. 19, pp. 15–32, 1 2005.

[33] D. P. Nedic, I. Dobson, D. S. Kirschen, B. A. Carreras, and V. E. Lynch, "Criticality in a cascading failure blackout model," *International Journal of Electrical Power and Energy Systems*, vol. 28, no. 9, pp. 627–633, 2006.

[34] Y. Guo, Z. Wang, S. Luo, and Y. Wang, "A cascading failure model for interdomain routing system," *International Journal of Communication Systems*, vol. 25, no. 8, pp. 1068–1076, 2012.

[35] S. Pahwa, A. Hodges, C. M. Scoglio, and S. Wood, "Topological analysis of the power grid and mitigation strategies against cascading failures," *CoRR*, vol. abs/1006.4627, 2010.