This paper will be presented at DRCN 2015 – 11th International Conference on Design of Reliable Communication Networks (March. 25–27, 2015, Kansas City, Missouri, USA)

Comprehensive Comparison and Accuracy of Graph Metrics in Predicting Network Resilience

Mohammed J.F. Alenazi*‡ and James P.G. Sterbenz*†
*Information and Telecommunication Technology Center
Department of Electrical Engineering and Computer Science
The University of Kansas, Lawrence, KS, 66045, USA
{malenazi, jpgs}@ittc.ku.edu
‡College of Computer and Information Sciences, Department of Computer Engineering
King Saud University, Riyadh, Saudi Arabia
†School of Computing and Communications (SCC) and InfoLab21
Lancaster LA1 4WA, UK
jpgs@comp.lancs.ac.uk
www.ittc.ku.edu/resilinets

***Abstract*—Graph robustness metrics have been used largely to study the behavior of communication networks in the presence of targeted attacks and random failures. Several researchers have proposed new graph metrics to better predict network resilience and survivability against such attacks. Most of these metrics have been compared to a few established graph metrics for evaluating the effectiveness of measuring network resilience. In this paper, we perform a comprehensive comparison of the most commonly used graph robustness metrics. First, we show how each metric is determined and calculate its values for baseline graphs. Using several types of random graphs, we study the accuracy of each robustness metric in predicting network resilience against centrality-based attacks. The results show three conclusions. First, our path diversity metric has the highest accuracy in predicting network resilience for structured baseline graphs. Second, the variance of node-betweenness centrality has mostly the best accuracy in predicting network resilience for Waxman random graphs. Third, path diversity, network criticality, and effective graph resistance have high accuracy in measuring network resilience for Gabriel graphs.**

***Keywords*—Network resilience;Network science;Connectivity evaluation;Graph robustness;Fault tolerance;Reliability; Survivability;Network design;Graph spectra**

I. Introduction and Motivation

The computer applications that rely on communication networks are critical to every aspect of our lives. Health care providers and receivers are becoming more dependent on computer networked applications [1]. E-learning is becoming an essential part of academic and professional education [2]. On-line businesses have an increasing number of customers. In 2014, the business-to-consumer (B2C) sales are estimated to be $1.5 trillion while this number is projected to increase in the upcoming years [3].

These networked services are publicly accessible, which make them prone to targeted attacks. Moreover, earthquakes, hurricanes, tsunami, and other natural disasters cause area-based node failures that not only affect local users but might significantly disrupt remote users. Computer network resilience is defined as the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation [4], [5]. Since computer networks are susceptible to targeted attacks and natural disasters that could disrupt its normal operation and services, building a network with higher resilience is a crucial part of its design and evolution.

In an attempt to provide a *good* network resilience measure, many researchers have proposed graph metrics that assess network robustness against nodes or links removal. For example, some *classic* graph metrics such as average node degree, clustering coëficcient, average hop count for shortest paths, radius, and diameter have been used to measure connectivity and robustness. k-connectivity – which indicates removing a minimum of k nodes to partition the graph – provides a good robustness measure against node failures. On the other hand, min-cut – which specifies the minimum number of links to partition a graph – provides a good robustness measure against link failures. These two metrics are promising robustness measures; however, the algorithmic complexity for these problems is NP-complete [6], which makes them intractable solutions for large networks.

Graph spectral theory studies the relationship between structural properties and *eigenvalues* and *eigenvectors* of their corresponding matrices. Several graph spectral metrics have been introduced to measure graph robustness against node or link removals. Such metrics are algebraic connectivity [7], spectral gap [8], natural connectivity [9], weighted spectrum [10], network criticality [11], and effective graph resistance [12]. Moreover, there have been several studies to compare a subset of these metrics [9], [13], [14]. The results of these metrics show promising ability to describe the robustness of a given graph.

In this paper, we compare the accuracy of several graph properties and graph robustness metrics to predict network resilience against targeted attacks. Using a set of baseline graphs, we calculate graph properties and robustness metrics for each graph to give the reader an intuition for how each metric is determined. Then, we present three resilience metrics to measure connectivity against centrality-based node attacks.

These metrics calculate the sum of *flow robustness*, which measures the number of remaining reliable flows during each attack [15]. The sum of the flow robustness values, while attacking all nodes, is our measure of network resilience because it captures the number of node-pair connections from start to the end of a given attack. Using a large set of randomly generated graphs, we check the accuracy of each graph robustness metric to predict graph resilience against centrality-based attacks. Our sample set consists of six classes of random graphs that exhibit similar graph properties of real-world communication networks. This sample set includes Waxman graphs, which have the mesh-like properties of logical level networks, and Gabriel graphs, which exhibit the grid-like properties of physical-level networks [16].

Our contribution in this work is twofold. First, we survey graph robustness metrics, which are used in the literature to predict network resilience against targeted attacks and random failures. Second, we present three network resilience measures against centrality-based attacks. Using baselines and random graphs, we study the accuracy of each spectra metric in predicting the three network resilience measures using a non-linear correlation.

The rest of the paper is organized as follows: review and discussion of related work is presented in Section II. A brief background on graph theory and several spectral graph robustness metrics are presented in Section III. A dataset of two types of graphs: baseline and random graphs, are explained in Section IV. The flow robustness metric, graph attack models, and measuring network resilience are presented in Section V. The results for evaluating the graph robustness metrics against each graph types are shown in Section VI. Finally, we summarize our findings as well as propose future work in Section VII.

II. Related Work

Several studies have been done to quantify graph robustness against targeted attacks and random failures. In this section, we present their work in terms of the proposed robustness metrics and how they have been evaluated.

Path diversity is a metric that measures disjoint nodes and links between alternative paths between two communicating nodes. The *total path diversity* (TGD) is the average path diversity among all node pairs [17]. The TGD has shown better accuracy in predicting survivability of synthetic and real networks when compared to other graph metrics such as clustering coëficcient, average hop count, and betweenness [17]. Furthermore, it has been shown that adding links to physical graphs to increase TGD provide better resilience than adding links to increase minimum degree nodes [18].

The variance of degree, closeness, and betweenness metrics have been used to quantify the centrality balance of a given graph. These graph metrics are proposed to measure graph robustness against targeted-node attacks [19]. Moreover, these metrics have been used as objective functions to improve graph robustness while adding a set of links to a given graph. The results show that degree-balanced improved graphs are more robust than betweenness- and closeness-balanced graphs against centrality-based attacks [19].

Algebraic connectivity has been studied by several researchers [20]–[22]. It has been shown that algebraic connectivity is more informative and accurate than average node degree when characterizing network resilience [21]. Another study improved synthetically generated Erdős-Rényi random and Barabási-Albert graphs in terms of adding links to the existing topology [20]. On the other hand, one study shows that algebraic connectivity is not tightly related to graph robustness via simulating node and link removals of several random graph types [23]. Moreover, we developed a heuristic algorithm that improves the connectivity of a graph using the algebraic connectivity metric by adding cost-efficient links in our earlier work [24], [25].

Weighted spectral distribution (WS) has been introduced to analyze the Internet topology [10]. Another study has been done to compare WS with other robustness metrics against geographic correlated failures and showed that WS is a better measure to evaluate geographically correlated vulnerable links and nodes [13].

Natural connectivity is a spectral graph metric that has been compared to algebraic connectivity using a set of structural and random graphs to examine robustness against node and link removals [9]. It has been shown that natural connectivity measures connectivity changes more precisely than algebraic connectivity.

Network criticality is a spectral graph metric that measures the robustness of a network against topological changes [11]. A smaller value of network criticality means higher network robustness. Furthermore, this metric has been compared to algebraic connectivity, average node degree, and average node betweenness. However, this study concluded that there is no unique graph metric that can capture robustness and connectivity [14].

The *spectral gap* is also a spectral graph metric that has been used to measure the robustness of the graph against targeted attacks [8]. A small spectral gap value indicates a smaller number of articulation points that might partition the network once a node or a link is removed [26].

Effective graph resistance is a spectral graph metric that measures the robustness of network against node or link removals [12]. This metric has been compared to algebraic connectivity in terms of measuring the connectivity of several random types and real-world networks.

III. Graph Robustness Metrics

In this section we present graph theoretic background and related work to network robustness metrics. Furthermore, we present graph spectra theory and its application to network robustness.

A. Graph Centrality Metrics

Graph centrality metrics show the importance of a link or a node to the graph. Since the node or link importance varies from one application to another, several metrics have been introduced as indicators to identify central nodes based on the need of the application [27].

The *node degree* centrality $\mathrm{C_D}(n)$, defined as the number of links incident to a node n and can be viewed as the node

importance [28]. The degree is a local centrality metric since it depends only on the number of links locally connected. *Assortativity* $\mathrm{As}(G)$ is a graph metric that measures the degree similarity among adjacent nodes for a given graph G [29]. For example, in a uniform-degree graph the assortativity is 1.

The *shortest path* $d_{i,j}$ between node i and node j is the path with the minimum number of hops. The *average shortest path length* $\bar{d}$ provides a measure of average number of hops among all nodes. Some other common graph metrics such as *eccentricity*, *radius*, and *diameter* provide statistical graph values of all node-pair shortest paths. The *eccentricity* $\varepsilon(v)$ is the longest of the shortest paths between node v and every other node. The graph *radius* $\mathrm{R}(G)$ is the *shortest* of the shortest paths of graph G. The graph *diameter* $\mathrm{D}(G)$ is the *longest* of the shortest paths of graph G.

Betweenness is a centrality metric that can be used for both nodes and links. Node betweenness $\mathrm{C_B}(n)$ is defined as the number of the shortest paths through a node n while link betweenness $\mathrm{C_B}(l)$ is defined as the number of the shortest paths through a link l. Betweenness is considered to have global significance since the betweenness value is impacted by the whole structure of the graph [30]. *Node closeness* $\mathrm{C_C}(n)$ is a centrality metric that measures the mean distance from the node n to other nodes [28], [31]. *Clustering coëficcient* $\mathrm{CC}(n)$ is a graph metric that measures how fully-connected a node's neighbors are [32].

B. Centrality-Balanced graph robustness

The high centrality nodes and links attract adversaries who can apply successful attacks on a targeted network by disrupting a few nodes with high centrality. For example a star network has one central node with high degree. Attacking this node completely disconnects the communication network. To measure the graph balanced-centrality property, four metrics have been introduced [19]. First, the degree-balanced graph metric $\sigma^2_{\mathrm{C_D}}$, which is computed as the degree variance of all the nodes. Second, closeness-balanced graph metric $\sigma^2_{\mathrm{C_C}}$, which is computed as the closeness variance of all the nodes. Third, node-betweenness-balanced graph metric $\sigma^2_{\mathrm{C_{B_v}}}$, which is computed as node-betweenness variance of all the nodes. Fourth, link-betweenness-balanced graph metric $\sigma^2_{\mathrm{C_{B_l}}}$, which is computed as node-betweenness variance of all the links.

C. Total Graph Diversity

Path diversity is defined as the ratio of the number of disjoint elements (nodes *and* links) between the shortest path and alternative path to the number of elements in the shortest path [17], [33]. Let the shortest path between a given (s, d) pair be P_0. Then, for any other path P_k the path diversity is computed as:

$$D(P_k) = 1 - \frac{|P_k \cap P_0|}{|P_0|} \tag{1}$$

The path diversity has a value of 1 if P_k and P_0 are completely disjoint and a value of 0 if P_k and P_0 are identical.

TGD (total graph diversity) is the average of the EPD (effective path diversity) values of all node pairs in a given graph [17] and TGD measures the structural path diversity of a graph as a single value. EPD is the normalized sum of path diversities for a selected set of paths connecting a node pair (s, d). The EPD value is calculated as:

$$\mathrm{EPD} = 1 - e^{-\lambda k_{sd}} \tag{2}$$

where λ is an experimentally determined constant that scales the impact of k_{sd} based on the utility of this added diversity [17] and k_{sd} is the sum of all non-zero diversity paths defined as:

$$k_{sd} = \sum_{i=1}^{m} D(P_i) \tag{3}$$

D. Graph Spectral Robustness Metrics

The topology of a graph G can be represented by an adjacency matrix, incidence matrix, Laplacian matrix, or normalized Laplacian matrix [34], [35]. Let $\{\mu_1, \mu_2, ..., \mu_n\}$ represent a non-decreasing list of the eigenvalues of the adjacency matrix and $\{\lambda_1, \lambda_2, ..., \lambda_n\}$ represent a non-decreasing list of the eigenvalues of the Laplacian matrix.

Algebraic connectivity, denoted as λ_2, is the second smallest eigenvalue of the Laplacian matrix [7] and defined as:

$$\lambda_2 \leq n(G) \leq l(G) \leq d_{\min}(G) \tag{4}$$

The algebraic connectivity $\lambda_2 = 0$ only if the graph is disconnected and $0 < \lambda_2 \leq N$ when the graph is connected.

Spectral gap, denoted as $\Delta\mu = \mu_n - \mu_{n-1}$, is the difference between the largest and the second largest eigenvalues of the adjacency matrix. Small spectral gap indicates articulation points that might partition the network once a node or a link is removed [26].

Natural connectivity, denoted as $\bar{\mu}$, is a scaled average eigenvalue of the graph adjacency matrix [9]. A larger value of $\bar{\mu}$ indicates higher robustness to link or node removals. The value of $\bar{\mu}$ is calculated as follows:

$$\bar{\mu} = \ln\left[\frac{1}{n}\sum_{j=1}^{n} e^{\mu_j}\right] \tag{5}$$

where μ is the jth eigenvalue of the adjacency matrix.

Weighted spectral distribution, denoted as WS, has been introduced to analyze Internet topology [10]. The value of WS is calculated as follows:

$$\mathrm{WS}(G, N) = \sum_{i=1}^{n} (1 - \lambda_i)^N \tag{6}$$

where λ_i is the ith eigenvalue of the Laplacian matrices and N is the number of cycles being measured [10]. In this paper, we use $N = 4$ since it is related to the number of disjoint paths [10], [13].

Network criticality, denoted as $\hat{\tau}$, is a graph metric that measures the robustness of network against topological changes [11]. A smaller value of $\hat{\tau}$ indicates higher network

robustness. We note that this metric is also called *total resistance distance* [36]. The value of $\hat{\tau}$ is calculated as follows:

$$\hat{\tau} = \frac{2}{|N|-1}\text{Trace}(L^{+}) \tag{7}$$

where $|N|$ is the number of nodes in a given graph, Trace(L^{+}) is the trace of the Moore-Penrose inverse of Laplacian matrix of the given graph [11].

Effective graph resistance, denoted as R_G, is a graph metric that measures the robustness of a network against node or link removals [12]. The value of R_G is calculated as follows:

$$\text{R}_G = N\sum_{i=2}^{N}\frac{1}{\lambda_i} \tag{8}$$

The normalized version is called *effective graph conductance* C^{*}, which is defined as:

$$\text{C}^{*} = \frac{N-1}{\text{R}_G} \tag{9}$$

where the values of C^{*} lie in the interval $[0, 1]$.

IV. Dataset

In this section, we present our datasets, which consists of two categories: *baseline* graphs and *random* graphs. For each category, we present several types and discuss graph properties. In all our models, we use simple undirected graphs, representation of bidirectional communication links.

A. Baseline graphs

We select a set of graphs with known structures to give some intuition of each graph metric during evaluation process. This set includes: *full-mesh*, *wheel*, *grid*, *torus*, *ladder*, *ring*, *barbell*, *linear*, *binary-tree*, and *star* graphs. A *full-mesh* graph, also called *complete*, has a link between every node pair. A *star* graph has one node designated as the root and a set of other nodes, while there is a link between the root and every other node. A *wheel* graph is a star graph with a link connecting all adjacent leaves. A *grid* graph has a $m \times n$ nodes placed in a grid form with m rows and n columns. In this graph, there is a link connecting every adjacent vertical and horizontal node pair. A *torus* graph is a grid graph with a link connecting every left and right nodes in each row and a link connecting every top and bottom nodes in each column. A *ladder* graph is a special case of the Grid graph such that n is always 2. A *linear* graph, also called a *path*, is a set of nodes placed as a line in which there is a link connecting every adjacent node pair. A *ring* graph, also called *circle*, is a linear graph with the end nodes connected by a link. A *binary-tree* graph has one node designated as a root with two children nodes. Each child has at most two children with a height h defining the length of the shortest path between the root and the leaves. A *barbell* has two full mesh graphs and a link connecting them. A set of examples for the baseline graphs are shown in Figure 1.

B. Random graphs

In this section, we present three random graph models to generate our dataset for robustness metrics evaluation.

1) Gilbert graphs: The Gilbert random graph model is one of the earliest models to construct random graphs [37]. Given a number of nodes n and connectivity probability p, the random graph model $\text{G}(n, p)$ constructs a graph with n nodes and m links are connected with probability p. Another similar graph model is the Erdős-Rényi (ER). The random graph model $\text{ER}(n, m)$ generates a graph with n nodes and randomly connected m links.

2) Waxman graphs: The Waxman model provides a probabilistic way of connecting nodes in a graph [38]. Given two nodes $\{u, v\}$ with a Euclidean distance $d(u, v)$ between them, the probability of connecting these two nodes is:

$$P(u, v) = \beta e^{\frac{-d(u,v)}{L\alpha}} \tag{10}$$

where $\beta, \alpha \in (0, 1]$ and L is the maximum distance between any two nodes. Increasing β increases the link density and a large value of α corresponds to a high ratio of long links to short links. In this paper, the Waxman model node locations are uniformly distributed.

3) Gabriel graphs: Gabriel graphs are useful in modeling graphs with geographic connectivity that resemble grids [39], [40]. In a Gabriel graph, two nodes are connected directly if and only if there are no other nodes that fall inside the circle whose diameter is given by the line segment joining the two nodes. The location of nodes are generated randomly using a uniform distribution with a range of $[0, 1]$ for both x-axis and y-axis. It has been shown that Gabriel graphs exhibit the grid-like properties of physical-level networks [16].

V. Measuring Robustness

In this section, we show how the flow robustness metric is determined. Then, we present our centrality-based attack models for robustness evaluation. Finally, we present three metrics to measure network resilience against centrality-based attacks.

A. Flow robustness

Flow robustness is a graph metric that measures the ratio of the number of reliable flows to the number of total flows in the network [15]. A flow is considered *reliable* if at least one of its paths remains unbroken by the link or node failures. The number of total flows is the maximum number of flows, which is $n(n-1)/2$ flows for n nodes. This metric captures the ability for the network nodes to communicate with each other. The range for flow robustness values is $[0, 1]$ where 1 indicates that all the nodes can communicate with each other and 0 means there is no node-pair communication in the whole network i.e. there are no links in the graph. The flow robustness metric can be used to model reachability, in which nodes communicate with each other. To calculate flow robustness, let $G = (N, L)$ be the graph representing the given network. Let $\{C_i; 1 < i < k\}$ be the set of components in graph G. The flow robustness FR is computed using:

$$\text{FR}(G) = \frac{\sum_{i=1}^{k}|C_i|(|C_i|-1)}{|n|(|n|-1)}, \qquad 0 \leq \text{FR} \leq 1 \tag{11}$$

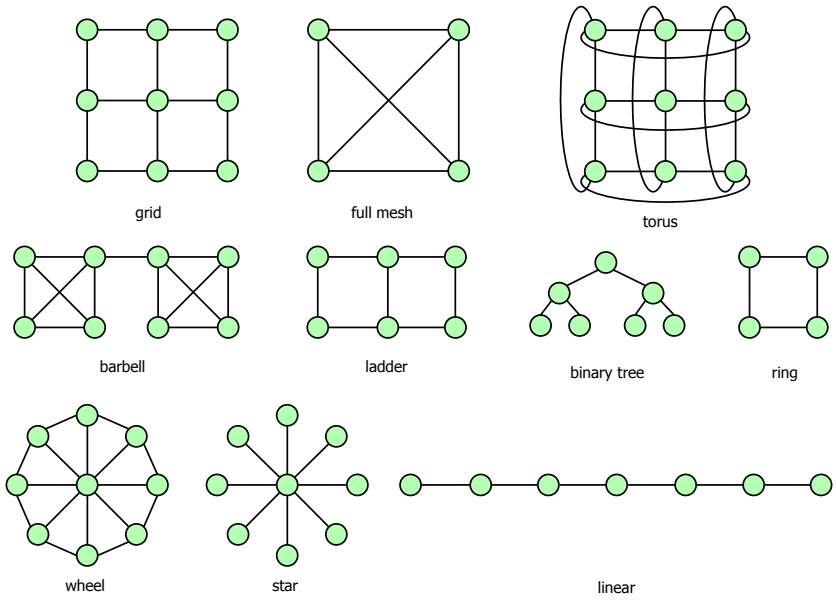

Fig. 1. Several example of baseline graphs

B. Graph attack models

We use a graph theoretic model to attack a given graph and show how its flow robustness changes after each node removal. In this paper, we use three centrality metrics: node betweenness, node closeness, and node degree [30]. Hence, we have three attack models, in which the node with the highest centrality is removed. The node-betweenness attack targets the node through which the highest number of shortest paths pass. The node-closeness attack targets the most central node in terms of hop count. The node-degree attack targets the node with the highest number of connections. If the attack requires removing multiple nodes, centrality metrics are recomputed upon attacking each node.

C. Measuring network resilience

In this section, we explain how to measure network resilience against a specific centrality-based attack. Flow robustness measures the reachability of a given graph. However, it is not useful to distinguish between *connected* graphs. For example, the flow robustness value for a full-mesh graph and a star graph is the same, which is one. As a solution, we introduce three robustness behavioral measures to calculate the sums of flow robustness of a given network resilience against centrality-based attacks. The robustness measures are: sums of flow robustness against degree attack (SFRD), sums of flow robustness against closeness attack (SFRC), and sums of flow robustness against betweenness attack (SFRB). Each measure captures resilience of a given network against the associated attack. For example, SFRD measures the network resilience against node degree-based attack.

Using an example, we illustrate how to measure network resilience of a 9-node wheel topology via sums of flow robustness against betweenness attack (SFRB). To compute the sums of flow robustness, we need to remove all nodes in this graph iteratively. In each iteration, one node is removed and the flow robustness is computed and added to the previous sum of flow robustness values. The permutation of nodes list define all possible ways for node attacks. In this example, we attack nodes based on their highest betweenness values, which yields the list $\{0, 1, 5, 3, 7, 8, 2, 4, 6\}$. Figure 2 depicts the topology while the attack is undergoing. Light green colored nodes indicate *connected* status (not attacked) while dark red colored nodes indicate *disconnected* status (attacked). Once a node is attacked all links attached to that node are removed. The values of robustness for each iteration are shown in the Table I. In step 2, we observe that after removing node 0, all 8 links are removed but flow robustness decreased by 0.22, which is not significant since there are alternative paths for the other nodes to communicate. However, in step 4, the flow robustness is decreased by $0.58 - 0.17 = 0.41$, which is the largest flow robustness decrease because the graph is partitioned into two components. Notice that we stop after step 6 since there are no remaining links and there is no need to attack the rest of the *connected* nodes. The sum of flow robustness values for a 9-node wheel topology is 2.61 as shown in the Table I.

TABLE I. MEASURING SFRB OF A 9-NODE WHEEL TOPOLOGY

Step	Removed Nodes	FR	SFRB
1	{}	1.00	1.00
2	{0}	0.78	1.78
3	{0, 1}	0.58	2.36
4	{0, 1, 5}	0.17	2.53
5	{0, 1, 5, 3}	0.08	2.61
6	{0, 1, 5, 3, 7}	0.00	2.61

VI. GRAPH METRICS EVALUATION

In this section, we present our evaluation results for baseline and random graphs. We show how each robustness metric is related to the resilience of a given graph against centrality-based attacks. To determine the accuracy of each graph metric in predicting the graph resilience against the three centrality-

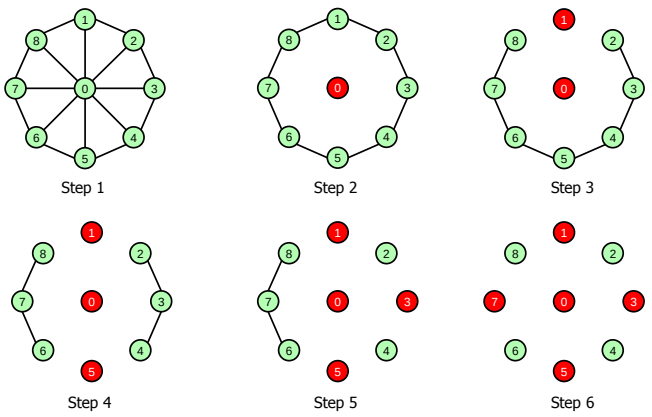

Fig. 2. Measuring SFRB a 9-node wheel topology

based attacks, we use a non-linear correlation function to check the graph metric and resilience measure dependency. In this paper, we use Spearman's rank correlation coefficient, which yields 1 for perfect correlation, -1 for perfect inverse correlation, and 0 for no correlation [41].

A. Baseline graphs

In this section, we generate 10 nodes in each graph presented in Section IV-A unless it is structurally impossible e.g. grid, torus, barbell, and tree graphs in which case we generate the feasible network closest to 10 nodes. Then, we apply the graph metrics presented in Section III and calculate their values for each generated baseline graph. Moreover, we measure the resilience of each graph against node attacks using the three measures SFRD, SFRC, and SFRB. The results are shown in Table II. For each metric, we measure its accuracy in predicting the resilience of the graphs by correlation of its values with resilience measures. For example, the *accuracy* of the metric number of links $|L|$ in *predicting* the resilience measure SFRD is 0.74. By observing all the correlation values for robustness metric X: corr(X, SFRD), corr(X, SFRC), and corr(X, SFRB), we notice that the total path diversity TGD graph metric has the highest accuracy values of 0.99, 0.96, 0.96 for corr(X, SFRD), corr(X, SFRC), and corr(X, SFRB) respectively. Next, we observe that node average degree places second with 0.91, 0.88, and 0.84 for the resilience measures. The third highest is variance of node-betweenness metric with accuracy values corr($\sigma^2_{C_{B_v}}$, SFRD | SFRC | SFRB) ≤ -0.85. Here the negative sign indicates an inverse correlation with robustness.

Among the presented graphs, the full-mesh graph has obviously the highest resilience since there is a link between every pair. On the other hand, the star graph has the lowest resilience because removing one node can fully disconnect the network. We observe that just the TGD and average node degree graph metrics capture this fact by ranking the full-mesh as the highest and the star as the lowest. Although algebraic connectivity and network criticality do not rank the mesh and star graphs correctly, their over all accuracy in predicting the resilience is higher, corr(λ_2, SFRD | SFRC | SFRB) ≥ 0.71 and corr($\hat{\tau}$, SFRD | SFRC | SFRB) ≤ -0.84, than the rest (except TGD and average node degree).

B. Random Graphs

In the baseline graphs evaluation, we have studied and compared 10 structurally different graphs to give some intuition about robustness metrics. However, with just 10 graphs, we can not draw a solid conclusion about the accuracy of the compared metrics to predict their resilience against node attacks. In this section, we increase our graph sample size from 10 graphs to 30,000 graphs divided into six 5000-sample-size classes. We note that all randomly generated graphs are all connected to avoid zero values for spectral robustness metrics. The number of nodes in each generated graph is 20. Using three corr(X, SFRD), corr(X, SFRC), and corr(X, SFRB), we calculate the accuracy of each graph metric to predict resilience using a sample of 5000 graphs. The correlation results are shown in Table III.

1) Gilbert graphs evaluation: The first two are Gilbert random graphs with $p = 0.8$ and $p = 0.5$. The Gilbert random graphs are completely random graphs that do not model real-world communication networks. By observing the correlation values of the all metrics for the three attacks, we see that all graph metrics have low accuracy in predicating network resilience i.e. | corr(X, SFRD | SFRC | SFRB) is mostly lower than 0.70. This is because of the complete randomness in generating Gilbert graphs. However, among the graph metrics, the $\sigma^2_{C_{B_v}}$ metric has slightly higher accuracy than the other metrics for degree and closeness attacks. Moreover, we observe that the algebraic connectivity λ_2 has the highest accuracy, corr(λ_2, SFRB)≥ 0.66 , in predicting graph resilience against betweenness attack (SFRB). On the other hand, we see that both radius and diameter graph properties have consistently the lowest accuracy in predicting network resilience for the two Gilbert graphs.

2) Waxman graphs evaluation: The next three random graphs are generated using Waxman models, W(α, β) , with three combination of parameters: $(\alpha = 0.5, \beta = 0.5)$, $(\alpha = 0.5, \beta = 0.8)$, and $(\alpha = 0.5, \beta = 0.8)$. Waxman graphs exhibit mesh-like properties that can model logical-level networks with some long links to reduce diameter. For the graphs with $\alpha = 0.5$ and $\beta = 0.5$, we get both medium density graphs and a medium number of long links. For the graphs with $\alpha = 0.5$ and $\beta = 0.8$, we get medium density graphs and a high number of long links. For the graphs with $\alpha = 0.8$ and $\beta = 0.5$, we get high density graphs and a medium number of long links. The maximum distance threshold L is set to 1 and the locations are randomly selected using a uniform distribution with a range of $[0, 1]$ for both x-axis and y-axis.

Unlike Gilbert graphs results, some Waxman graph metrics have high accuracy values in measuring resilience. We observe that the variance of the node-betweenness metric has slightly higher accuracy than the others metrics for degree and closeness attacks i.e. corr($\sigma^2_{C_{B_n}}$, SFRD | SFRC) ≤ -0.75. Next, both network criticality $\hat{\tau}$ and effective graph resistance C^* are the second best predictors for graph resilience against both degree and closeness attacks. In fact, both metrics have *almost* identical accuracy results because they both claim to measure *graph resistance* using the eigenvalues of Laplacian matrix.

For betweenness attacks, both network criticality $\hat{\tau}$ and effective graph resistance C* are the best predictor for graph resilience with corr($\hat{\tau}$, SFRB)≤ -0.78. We also note that both

TABLE II. EVALUATING GRAPH ROBUSTNESS METRICS USING BASELINE GRAPHS

	Barbell	Grid	Ladder	Linear	Mesh	Ring	Star	Torus	Tree	Wheel	corr(X, SFRD)	corr(X, SFRC)	corr(X, SFRB)
$\|N\|$	12.00	9.00	10.00	10.00	10.00	10.00	10.00	9.00	15.00	10.00	—	—	—
$\|L\|$	17.00	12.00	13.00	9.00	45.00	10.00	9.00	18.00	14.00	18.00	0.68	0.79	0.74
$\bar{C_D}$	2.83	2.67	2.60	1.80	9.00	2.00	1.80	4.00	1.87	3.60	0.84	0.88	0.91
$\sigma^2_{C_D}$	0.47	0.44	0.24	0.16	0.00	0.00	5.76	0.00	0.92	3.24	-0.58	-0.48	-0.55
$\sigma^2_{C_C}$	0.00	0.00	0.00	0.00	0.00	0.00	0.02	0.00	0.00	0.01	-0.43	-0.40	-0.44
$\sigma^2_{C_{Bv}}$	0.06	0.01	0.01	0.04	0.00	0.00	0.09	0.00	0.05	0.03	-0.88	-0.85	-0.85
$\sigma^2_{C_{Bl}}$	0.04	0.00	0.00	0.02	0.00	0.00	0.00	0.00	0.02	0.00	-0.56	-0.54	-0.54
CC	0.58	0.00	0.00	0.00	1.00	0.00	0.00	0.33	0.00	0.62	0.60	0.60	0.66
As	0.13	-0.06	0.28	-0.12	1.00	1.00	-1.00	1.00	-0.52	-0.33	0.66	0.61	0.68
R	4.00	2.00	3.00	5.00	1.00	5.00	1.00	2.00	3.00	1.00	-0.38	-0.46	-0.40
D	7.00	4.00	5.00	9.00	1.00	5.00	2.00	2.00	6.00	2.00	-0.60	-0.65	-0.62
$\bar{d}$	3.48	2.00	2.33	3.67	1.00	2.78	1.80	1.50	3.50	1.60	-0.71	-0.73	-0.73
TGD	0.23	0.73	0.68	0.00	1.00	0.39	0.00	0.91	0.00	0.82	0.96	0.96	0.99
λ_2	0.09	1.00	0.38	0.10	10.00	0.38	1.00	3.00	0.10	1.47	0.81	0.78	0.78
$\Delta\lambda$	0.01	1.41	0.73	0.24	10.00	0.38	3.00	3.00	0.29	2.63	0.58	0.60	0.57
$\hat{\tau}$	3.03	0.96	1.25	3.67	0.20	1.83	1.80	0.50	3.50	0.69	-0.84	-0.87	-0.87
WS	3.02	2.44	3.04	4.37	1.00	3.75	2.00	1.27	5.46	1.48	-0.67	-0.65	-0.71
$\bar{\lambda}$	2.19	1.67	1.61	1.09	9.66	1.19	1.49	2.87	1.18	2.95	0.75	0.77	0.82
C^*	0.06	0.23	0.16	0.05	1.00	0.11	0.11	0.44	0.04	0.29	0.87	0.84	0.88
SFRD	1.97	2.72	2.62	2.11	3.67	2.56	1.00	3.14	1.61	2.91	1.00	0.95	0.99
SFRC	1.86	2.61	2.47	1.67	3.67	2.29	1.00	3.14	1.94	2.73	0.95	1.00	0.96
SFRB	1.86	2.61	2.47	1.67	3.67	2.29	1.00	3.14	1.61	2.73	0.99	0.96	1.00

TABLE III. EVALUATING GRAPH ROBUSTNESS METRICS USING RANDOM GRAPHS

	$\|L\|$	$\bar{C_D}$	$\sigma^2_{C_D}$	$\sigma^2_{C_C}$	$\sigma^2_{C_{Bn}}$	$\sigma^2_{C_{Bl}}$	CC	As	R	D	$\bar{d_{ij}}$	TGD	λ_2	$\Delta\lambda$	$\hat{\tau}$	WS	$\bar{\lambda}$	C^*
corr(X, SFRD)																		
Gilbert p=0.8	0.44	0.44	-0.43	-0.33	-0.53	-0.47	0.36	0.38	0.21	0.00	-0.42	0.53	0.47	0.39	-0.45	-0.47	0.41	0.47
Gilbert p=0.5	0.54	0.54	-0.38	-0.27	-0.66	-0.53	0.31	0.40	0.00	-0.04	-0.54	0.47	0.53	0.39	-0.61	-0.52	0.47	0.61
$W(0.5, 0.5)$	0.75	0.75	-0.06	-0.35	-0.81	-0.69	0.25	0.30	-0.12	-0.33	-0.70	0.74	0.63	0.43	-0.79	-0.66	0.61	0.79
$W(0.5, 0.8)$	0.68	0.68	-0.24	-0.49	-0.78	-0.68	0.23	0.35	0.13	-0.24	-0.67	0.67	0.64	0.42	-0.76	-0.60	0.55	0.76
$W(0.8, 0.5)$	0.63	0.63	-0.25	-0.47	-0.75	-0.64	0.24	0.33	0.43	0.15	-0.64	0.60	0.61	0.39	-0.73	-0.57	0.51	0.73
Gabriel	0.65	0.65	0.12	-0.01	-0.49	-0.50	0.26	0.14	-0.12	-0.31	-0.55	0.70	0.53	0.15	-0.66	-0.60	0.56	0.66
corr(X, SFRC)																		
Gilbert p=0.8	0.45	0.45	-0.44	-0.33	-0.54	-0.47	0.37	0.39	0.21	0.00	-0.42	0.54	0.49	0.40	-0.45	-0.47	0.42	0.48
Gilbert p=0.5	0.52	0.52	-0.35	-0.25	-0.64	-0.52	0.27	0.37	0.00	-0.04	-0.52	0.44	0.51	0.40	-0.58	-0.50	0.45	0.58
$W(0.5, 0.5)$	0.73	0.73	-0.02	-0.35	-0.83	-0.73	0.20	0.20	-0.12	-0.33	-0.71	0.72	0.64	0.46	-0.78	-0.67	0.60	0.78
$W(0.5, 0.8)$	0.68	0.68	-0.20	-0.50	-0.78	-0.71	0.18	0.26	0.13	-0.24	-0.68	0.67	0.65	0.46	-0.76	-0.61	0.55	0.76
$W(0.8, 0.5)$	0.63	0.63	-0.20	-0.45	-0.75	-0.66	0.20	0.27	0.43	0.16	-0.64	0.58	0.60	0.44	-0.71	-0.57	0.51	0.71
Gabriel	0.61	0.61	0.17	0.02	-0.58	-0.65	0.17	0.12	-0.15	-0.36	-0.62	0.71	0.65	0.27	-0.71	-0.58	0.52	0.71
corr(X, SFRB)																		
Gilbert p=0.8	0.43	0.43	-0.60	-0.41	-0.61	-0.69	0.32	0.25	0.15	0.00	-0.43	0.59	0.75	0.37	-0.49	-0.46	0.39	0.49
Gilbert p=0.5	0.49	0.49	-0.43	-0.29	-0.62	-0.64	0.23	0.28	0.00	-0.09	-0.50	0.42	0.69	0.33	-0.60	-0.46	0.40	0.60
$W(0.5, 0.5)$	0.76	0.76	-0.03	-0.40	-0.84	-0.81	0.22	0.15	-0.16	-0.41	-0.77	0.81	0.74	0.45	-0.85	-0.72	0.60	0.85
$W(0.5, 0.8)$	0.67	0.67	-0.24	-0.56	-0.78	-0.79	0.18	0.20	0.11	-0.31	-0.71	0.74	0.75	0.42	-0.81	-0.62	0.52	0.81
$W(0.8, 0.5)$	0.62	0.62	-0.26	-0.54	-0.73	-0.78	0.19	0.16	0.42	0.11	-0.68	0.66	0.76	0.39	-0.78	-0.58	0.48	0.78
Gabriel	0.62	0.62	0.18	0.06	-0.53	-0.68	0.17	0.10	-0.22	-0.43	-0.69	0.73	0.73	0.27	-0.77	-0.61	0.51	0.77

$\sigma^2_{C_{Bl}}$ and TGD metrics have the second- and third-best results respectively for the betweenness attack. Moreover, we observe that the radius graph property *generally* performs very poorly in predicting the graph resilience.

3) Gabriel graphs evaluation: The sixth random graph class is generated using Gabriel graphs that exhibit grid-like structure and model physical-level networks. By observing the correlation values of the all metrics for the three attacks, we see that the total path diversity TGD has the best accuracy values for predicting network resilience against both degree and closeness attacks with corr(TGD, SFRD | SFRC)≥ 0.70. For the betweenness attack, we see that both $\hat{\tau}$ and C^* are the best predictors for graph resilience.

VII. CONCLUSIONS AND FUTURE WORK

Computer networks are prone to targeted attacks and random failures. Evaluating and improving communication networks resilience against these is an important aspect of network design. In this paper, we evaluate a set of graph robustness metrics to measure their accuracy in predicting network resilience against centrality-based attacks via baseline and random graphs. For baseline graphs, we show that the path diversity metric has a high accuracy in predicting network resilience. Generally, the variance of node-betweenness centrality has the highest accuracy. For Waxman graphs, which resemble logical-level networks, the variance of node-betweenness centrality metric has the highest accuracy for degree- and closeness-based attacks while network criticality $\hat{\tau}$ and effective graph resistance C^* have better results for betweenness-based attack. All path diversity, network criticality, and effective graph resistance have high accuracy in measure network resilience centrality-based attacks for Gabriel graphs, which resemble physical-level network. For future work, we plan to evaluate weighted graph metrics and see how our unweighted graph evaluation results compare to evaluating weighted graphs. In addition, we plan to evaluate these robustness metrics using larger order random graphs and real service provider networks.

ACKNOWLEDGMENTS

We would like to acknowledge Dongsheng Zhang and Yufei Cheng for discussions on this work. This research was supported in part by NSF grant CNS-1219028 (Resilient Network Design for Massive Failures and Attacks) and by NSF grant CNS-1050226 (Multilayer Network Resilience Analysis and Experimentation on GENI). Mohammed J.F. Alenazi is supported by in part SACM (Saudi Arabian Cultural Mission) and King Saud University.

REFERENCES

[1] R. L. Street, W. R. Gold, and T. R. Manning, *Health promotion and interactive technology: Theoretical applications and future directions*. Routledge, 2013.

[2] D. Zhang, J. L. Zhao, L. Zhou, and J. F. Nunamaker Jr, "Can e-learning replace classroom learning?," *Communications of the ACM*, vol. 47, no. 5, pp. 75–79, 2004.

[3] "Global B2C Ecommerce Sales to Hit $1.5 Trillion This Year Driven by Growth in Emerging Markets - eMarketer."

[4] J. P. G. 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.

[5] ENISA Virtual Working Group on Network Providers Resilience Measures, "Network resilience and security: Challenges and measures," Tech. Rep. WP 2009 – WPK 1.2 VWG 1, ENISA – European Network and Information Security Agency, December 2009.

[6] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*. New York, NY, USA: W. H. Freeman & Co., 1979.

[7] M. Fiedler, "Algebraic connectivity of graphs," *Czechoslovak Mathematical Journal*, vol. 23, no. 2, pp. 298–305, 1973.

[8] E. Estrada, "Network robustness to targeted attacks. the interplay of expansibility and degree distribution," *The European Physical Journal B-Condensed Matter and Complex Systems*, vol. 52, no. 4, pp. 563–574, 2006.

[9] J. Wu, M. Barahona, Y.-J. Tan, and H.-Z. Deng, "Spectral measure of structural robustness in complex networks," *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, vol. 41, no. 6, pp. 1244–1252, 2011.

[10] D. Fay, H. Haddadi, A. Thomason, A. Moore, R. Mortier, A. Jamakovic, S. Uhlig, and M. Rio, "Weighted Spectral Distribution for Internet Topology Analysis: Theory and Applications," *IEEE/ACM Transactions on Networking*, vol. 18, no. 1, pp. 164–176, 2010.

[11] A. Tizghadam and A. Leon-Garcia, "Autonomic traffic engineering for network robustness," *Selected Areas in Communications, IEEE Journal on*, vol. 28, no. 1, pp. 39–50, 2010.

[12] X. Wang, E. Pournaras, R. E. Kooij, and P. Van Mieghem, "Improving robustness of complex networks via the effective graph resistance," *The European Physical Journal B*, vol. 87, no. 9, pp. 1–12, 2014.

[13] X. Long, D. Tipper, and T. Gomes, "Measuring the survivability of networks to geographic correlated failures," *Optical Switching and Networking*, vol. 14, Part 2, no. 0, pp. 117 – 133, 2014.

[14] A. Bigdeli, A. Tizghadam, and A. Leon-Garcia, "Comparison of network criticality, algebraic connectivity, and other graph metrics," in *Proceedings of the 1st Annual Workshop on Simplifying Complex Network for Practitioners*, p. 4, ACM, 2009.

[15] J. P. Rohrer, A. Jabbar, and J. P. G. Sterbenz, "Path diversification: A multipath resilience mechanism," in *Proceedings of the IEEE 7th International Workshop on the Design of Reliable Communication Networks (DRCN)*, (Washington, DC), pp. 343–351, October 2009.

[16] E. K. Cetinkaya, M. J. Alenazi, Y. Cheng, A. M. Peck, and J. P. Sterbenz, "A comparative analysis of geometric graph models for modelling backbone networks," *Optical Switching and Networking*, vol. 14, Part 2, pp. 95 – 106, 2014.

[17] J. P. Rohrer, A. Jabbar, and J. P. Sterbenz, "Path Diversification for Future Internet End-to-End Resilience and Survivability," *Springer Telecommunication Systems*, vol. 56, pp. 49–67, May 2014.

[18] M. J. Alenazi, E. K. Çetinkaya, and J. P. G. Sterbenz, "Cost-Efficient network improvement to achieve maximum path diversity," in *RNDM'14 - 6th International Workshop on Reliable Networks Design and Modeling (RNDM 2014)*, (Barcelona, Spain), pp. 202 – 208, Nov. 2014.

[19] M. J. Alenazi, E. K. Çetinkaya, and J. P. G. Sterbenz, "Cost-Constrained and Centrality-Balanced network design improvement," in *RNDM'14 - 6th International Workshop on Reliable Networks Design and Modeling (RNDM 2014)*, (Barcelona, Spain), pp. 194 – 201, Nov 2014.

[20] H. Wang and P. Van Mieghem, "Algebraic connectivity optimization via link addition," in *Proceedings of the 3rd ICST International Conference on Bio-Inspired Models of Network, Information and Computing Sytems (BIONETICS)*, (Hyogo, Japan), pp. 22:1–22:8, November 2008.

[21] W. Liu, H. Sirisena, K. Pawlikowski, and A. McInnes, "Utility of algebraic connectivity metric in topology design of survivable networks," in *Proceedings of the 7th IEEE International Workshop on Design of Reliable Communication Networks (DRCN)*, (Washington, DC), pp. 131–138, October 2009.

[22] A. Sydney, C. Scoglio, and D. Gruenbacher, "Optimizing algebraic connectivity by edge rewiring," *Applied Mathematics and Computation*, vol. 219, no. 10, pp. 5465–5479, 2013.

[23] A. Jamaković and S. Uhlig, "On the relationship between the algebraic connectivity and graph's robustness to node and link failures," in *Proceedings of the 3rd EuroNGI Conference on Next Generation Internet Networks*, (Trondheim), pp. 96–102, May 2007.

[24] M. J. F. Alenazi, E. K. Çetinkaya, and J. P. G. Sterbenz, "Network Design and Optimisation Based on Cost and Algebraic Connectivity," in *Proceedings of the 5th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM)*, (Almaty), pp. 193–200, September 2013.

[25] M. J. Alenazi, E. K. Çetinkaya, and J. P. Sterbenz, "Cost-efficient algebraic connectivity optimisation of backbone networks," *Optical Switching and Networking*, vol. 14, Part 2, pp. 107 – 116, 2014.

[26] A. Yazdani, R. A. Otoo, and P. Jeffrey, "Resilience enhancing expansion strategies for water distribution systems: A network theory approach," *Environmental Modelling & Software*, vol. 26, no. 12, pp. 1574–1582, 2011.

[27] L. d. F. Costa, F. A. Rodrigues, G. Travieso, and P. R. Villas Boas, "Characterization of complex networks: A survey of measurements," *Advances in Physics*, vol. 56, no. 1, pp. 167–242, 2007.

[28] L. C. Freeman, "Centrality in social networks conceptual clarification," *Social Networks*, vol. 1, no. 3, pp. 215–239, 1978–1979.

[29] M. E. J. Newman, "Assortative mixing in networks," *Phys. Rev. Lett.*, vol. 89, p. 208701, October 2002.

[30] L. C. Freeman, "A Set of Measures of Centrality Based on Betweenness," *Sociometry*, vol. 40, no. 1, pp. 35–41, 1977.

[31] M. E. J. Newman, *Networks: An Introduction*, ch. 7, p. 199. Oxford University Press, 1st ed., 2010.

[32] H. Haddadi, M. Rio, G. Iannaccone, A. Moore, and R. Mortier, "Network Topologies: Inference, Modeling, and Generation," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 2, pp. 48–69, 2008.

[33] M. Motiwala, M. Elmore, N. Feamster, and S. Vempala, "Path Splicing," in *Proceedings of the ACM SIGCOMM*, (Seattle, WA), pp. 27–38, August 2008.

[34] F. R. K. Chung, *Spectral Graph Theory*. American Mathematical Society, 1997.

[35] P. Van Mieghem, *Graph Spectra for Complex Networks*. Cambridge University Press, 2011.

[36] A. Tizghadam and A. Leon-Garcia, "Betweenness centrality and resistance distance in communication networks," *Network, IEEE*, vol. 24, no. 6, pp. 10–16, 2010.

[37] E. N. Gilbert, "Random graphs," *The Annals of Mathematical Statistics*, pp. 1141–1144, 1959.

[38] B. M. Waxman, "Routing of Multipoint Connections," *IEEE Journal on Selected Areas in Communications*, vol. 6, no. 9, pp. 1617–1622, 1988.

[39] K. R. Gabriel and R. R. Sokal, "A New Statistical Approach to Geographic Variation Analysis," *Systematic Zoology*, vol. 18, no. 3, pp. 259–278, 1969.

[40] D. W. Matula and R. R. Sokal, "Properties of Gabriel Graphs Relevant to Geographic Variation Research and the Clustering of Points in the Plane," *Geographical Analysis*, vol. 12, no. 3, pp. 205–222, 1980.

[41] C. Spearman, "The proof and measurement of association between two things," *The American Journal of Psychology*, vol. 15, no. 1, pp. pp. 72–101, 1904.