Analyzing Transmission Lines Robustness and Resilience Prediction Accuracy with Line Graph Based Model

Aiman Albarakati, Marwan Bikdash
Department of Computational Science and Engineering
North Carolina A&T State University
Greensboro, USA

***Abstract*—We examine the resilience prediction accuracy of differential centrality and spectral graph measurements, applied to a power systems line-graph based model (LGBM). We test LGBM robustness and related metrics using IEEE test cases. We consider predictive resilience for the LGBM of different IEEE systems. and analyze the accuracy of Sum of Flow Robustness when facing Degree-based attacks (SFRD) and we introduce the Sum of Flow Robustness facing Eigenvalue-based attacks (SFRE). Results show that number of links, average path length, and radius, provide accurate predictions for resilience. We use the weighted networks based on admittance matrix (electrical characteristics) to predict the resilience based on BBM and LGBM. Results show that clustering coefficient, provides accurate predictions for resilience in BBM weighted network, and average path length provides accurate predictions for resilience in LGBM weighted network.**

Keywords—Power systems robustness, line graphs, transmission lines resilience, complex networks.

I. INTRODUCTION

In recent years, the study of power systems robustness against events such as failures that can damage network integrity, has received increased interest [1], [2]. Various models have been applied to assess the vulnerability of the power grid and its resilience against such events. For example, Carreras, and Lynch [3] employed a tree-structured power grid model to investigate the strength of a power network against attack. This model also identified phase changes, transitions and critical points in the transmission network. Complex network and graph theories are often applied to power grids, particularly for assessment of robustness, risk and vulnerability against failures [4]–[8]. Several reviews have attempted to quantify the robustness of power systems graphs against focused or targeted attacks and arbitrary failures [10]–[12]. To measure the centrality of graph nodes, these reviews analyze variation in node degree, node betweeness, and node proximity. These graph-based metrics have then been used as determinants for graph-based robustness against targeted attacks to nodes. In addition to adding an arrangement of connections/links to a given graph, these measurements have further been presented as target capacities for optimum graph robustness. Across the literature [13]-[18], findings demonstrate that when facing targeted attacks, graphs enhanced with balancing degrees are less vulnerable than are those with balanced betweeness and closeness centralities. Considering algebraic connectivity, findings indicate that 'network resilience' is a more appropriate descriptor [13], [14]. Other spectral graph metrics commonly employed to determine network robustness are effective graph resistance and network criticality; the first is against node or link removals, and the second against topological variations [12], [15] The above studies focus on bus-based models of power systems [16]–[18], however, they do not pay attention to transmission lines. Considering this gap in the research, we proposed a line-graph based model (LGBM) in our previous work [35] to assess the vulnerability of power systems as part of complex network theory. For each LGBM, IEEE test cases were used to obtain graph properties and robustness metrics. Then, to estimate connectivity following centrality-based node attacks . One of these measures, sum of flow robustness, quantifies the reliable flows remaining after the attack. In this research we introduced Sum of Flow Robustness based on Eigenvalue centrality (SFRE) resilience metrics and compare the results with Sum of Flow Robustness based on degree centrality (SFRD) that introduced in [12] . Using the Sum of Flow Robustness obtained after each attack on different IEEE test cases, we inspected the accuracy of each metric to predict resilience against centrality-based attacks. In this work we identified the best predictor metrics for the LGBM networks problems, computed and compared graph metrics of the weight networks where the weights are based on electrical characteristics. This paper is organized as follows: In Section II we examine a mathematical LGBM for robustness. In Section III, computing the graph theoretic for BBM and LGBM . In Section IV, we predict the resilience of BBM and LGBM for unweighted networks based on SFRD and SFRE. In section V we reproduce section VI to predict the resilience based on weighted networks for Bus Based Model BBM and Line Graph Based Model LGBM based on SFRD and SFRE . Finally, in Section VI we provide a summary of our findings .

II. LINE GRAPH BASED MODEL FOR ROBUSTNESS

A. Review of electrical Flow equation[34]

The function of a power system can be described by its admittance matrix Y, power-generation data, power consumption, and device capacity. The Y matrix of the grid governs

978-1-5386-6133-8/18/$31.00 ©2018 IEEE

the power flow in the system, and it depends on the topology of the network. The power network dynamics are governed by following the network equations [36][37]:

$$I = Y_{bus}V, \tag{1}$$

where Y_{bus} is the $m \times m$ admittance matrix, I is the vector of injected currents in each node , V_{bus} is the vector of complex bus voltages, and Y^L representing admittance of busses to ground.

The matrix can be further divided into two parts, Y representing the matrix of admittance between busses and Y^L representing admittance of busses to ground as shows :

$$I = (Y + Y^L)V. \tag{2}$$

The off-diagonal elements of Y is equal to the negative of the admittance between the nodes. It is known as the mutual admittance or transfer admittance, i.e.,

$$Y = G + \mathbf{j}B \in \mathbb{R}^{m\times m} \tag{3}$$

$$: \begin{cases} Y_{ii} = \sum_{k=1}^{\mathrm{n}} \bar{y}_{ik} & \text{for k=i,} \\ Y_{ik} = Y_{ki} = -\bar{y}_{ik} & \text{for k}\neq\text{i.} \end{cases} \tag{4}$$

where G is the conductance matrix, B is the susceptance matrix, and $\bar{y}_{ik}$ is the admittance for the transmission line $l(i,j)$ between buses i and j. Assuming that the system has m busses and n transmission lines connecting those buses, the admittance matrix Y is of size $m \times m$ and is determined by the topology and the electrical characteristics of transmission lines. Each transmission line $l(i,j)$, has a line impedance corresponding to $z(l) = r(l)+jx(l)$, in which $r(l)$ is resistance and $x(l)$ reactance. Line admittance can be calculated from the inverse of the impedance, as shown in the following:

$$y(l) = \frac{1}{z(l)} = g(l) + jb(l). \tag{5}$$

In power networks, reactance often dominates resistance, and typically $b(l) >> g(l)$. Considering current of 1 per unit flowing through the transmission line $l(i,j)$, deviation of the voltage between extremes of the transmission line is $\Delta v = V(i) - V(j) = z(l)$, or equivalently, $\Delta v = 1/y(l)$[34].

Hence, link impedance can be understood as a measure of electrical distance or separation between busses, and admittance measures $y(l)$, as a measure of coupling between busses.

Using(1), and (3),the complex power injected in to bus $\bar{S}_{bus}$ is given by the following : [34]

$$\bar{S}_i = P_i + jQ_i = V_i I_i^*,$$

$$\bar{S}_k = V_i(\sum_{k=1,k\neq i}^{N_b} Y_{ik}V_k)^* + y_{ii}^{*L} V_i V_i^*.$$

B. Review of Graph theoritical description[35]

This section reviews facts from graph theory that are well known and are summarized here from [35]. A graph $G(V,E)$ has a set of nodes V and a set of links or edges E. A rather complete description of the graph is in terms of the so called incidence matrix [7], which is $m \times n$ matrix C. Here we use the unoriented version which works well for undirected graphs. It is defined as

$$C : \begin{cases} c_{il} = 1 & \text{if link } l \text{ is incident on node } i \text{ in } G, \\ c_{il} = 0 & \text{otherwise.} \end{cases} \tag{6}$$

Here C is an $m \times n$ matrix with m being the number of nodes and n is the number of edges. The oriented incidence matrix B assumes directed edges, is given by[35]

$$B : \begin{cases} b_{il} = -1 & \text{if link } l \text{ ends at node } i \text{ in } G, \\ b_{il} = 1 & \text{if link } l \text{ starts at node } i \text{ in } G, \\ b_{il} = 0 & \text{otherwise.} \end{cases} \tag{7}$$

For a Bus Based Model (BBM) , a graph G is defined where nodes are buses and edges are transmission lines. There is a relationship between admittance matrix Y and the adjacency and incidence matrices as follows:

$$Y = B\Gamma B^T, \tag{8}$$

where B is the bus oriented incidence matrix and Γ is the primitive admittance matrix, where Γ defined as :

$$\Gamma = [diag(\gamma_e)], \tag{9}$$

where γ_e is the admittance of e^{th} link .The element (i,j) of the matrix Γ is the admittance of the i^{th} branch of the network G.

For undirected graphs, the signs can be assigned arbitrarily, typically with no important implications. Obviously, the unoriented incidence matrix can be obtained from the oriented incidence matrix by dropping the signs.

The adjacency matrix $A \in \{0,1\}^{m\times m}$ of G is defined as [7][35]

$$A : \begin{cases} a_{ij} = 1 & \text{if node } i \text{ shares a link with node } j \text{ in } G, \\ a_{ij} = 0 & \text{otherwise.} \end{cases} \tag{10}$$

It can be shown that the adjacency matrix can be computed from the oriented incidence matrix as follows [7]

$$A := D - BB^T, \tag{11}$$

where D is degree matrix. This is a diagonal matrix where d_{ii} is the degree of node i

$$d_{ii} = \sum_{j=1}^{m} a_{ij}, \tag{12}$$

In other word, is the number of links in G that are incident on node i. The degree distribution $P(k)$ is the portion of nodes from the graph that have a degree k [22]. For large stochastic networks, this is the probability that a node selected randomly has k edges. Degree distribution is useful to identify the network type and to understand vulnerability according to the corresponding model. For instance, the degree distribution of a random network is a Poisson probability distribution.

The adjacency matrix A^L of the corresponding line graph $G' = L(G)$ can be stated in terms of the unoriented incidence matrix C of the original graph G as [20][35]

$$A^L = C^T C - 2I_n, \tag{13}$$

where I_n is the $n \times n$ matrix. Clearly it relates the edges of the original graph. In fact, if $a_{ij}^L = 1$, then [35]

$$\begin{cases} \text{edges } i \text{ and } j \text{ in } G \text{ share a node,} \\ \text{nodes } i \text{ and } j \text{ in } G' = L(G) \text{ share an edge.} \end{cases} \tag{14}$$

C. Weighted Graph description of Power networks

To model the power system as a weighted graph $\tilde{G}$ weighted BBM, the weighted adjacency matrix $\tilde{A}$ is obtained from the admittance matrix as follows

$$\tilde{A} : \begin{cases} \tilde{a}_{ij} = w_{ij} & \text{if node } i \text{ shares a link with node } j \text{ in } \tilde{G}, \\ \\ \tilde{a}_{ij} = 0 & \text{otherwise.} \end{cases} \tag{15}$$

where $w \in \mathbb{R}^{\mathrm{m}}$ represents the weight on the edge in $\tilde{G}$, in this research $w_{ij} = y_{ij}$ represents the admittance of branch $l(i,j)$. To get the sum of the weights $\tilde{k}$ of each node adjacent edges in $\tilde{G}$ we use the following :

$$\tilde{k} = \tilde{A} 1_n. \tag{16}$$

The matrix $\tilde{D}$ is a diagonal matrix of $\tilde{k}$ in (16) by using the following

$$\tilde{D} = \mathrm{diag}(\tilde{k}). \tag{17}$$

We define weighted unoriented incidence matrix $\tilde{C}$ based on $\tilde{G}$ as follows :

$$\tilde{C} : \begin{cases} c_{il}^w = w_{ij} & \text{if link } l \text{ is incident on node } i \text{ in } \tilde{G}, \\ c_{il}^w = 0 & \text{otherwise.} \end{cases} \tag{18}$$

where link $l(i,j)$ is adjacent to node i and node j.

According to [20] the equivalent Naive adjacency matrix for weighted line graphs is derived as following :

$$\tilde{E} = \tilde{C}^T \tilde{D}^{-1} \tilde{C}, \tag{19}$$

where $\tilde{C}^T$ is the transpose of the weighted incidence matrix $\tilde{C}$ in (18) .

The weighted line graph is characterized by the Naive adjacent matrix $\tilde{E}$; they can be calculated using (19) . These equivalent matrices called Naive because it possess self-loops, which can be eliminated by removing non-zero diagonal components. To eliminate self-loops, Yoshida [20] suggests dispersing the non-zero diagonal components of the original matrix, for instance $\tilde{E}$, although, it should be noted that some properties are preserved. To calculate the transformed matrix, the vector e comprises the diagonal elements of $\tilde{E}$ as the following:

$$e = (\mathrm{diag}(\tilde{E})), \tag{20}$$

the D_E matrix is a diagonal matrix with e as elements as follows:

$$D_E = \mathrm{diag}(e), \tag{21}$$

the matrix $\tilde{E}_1$ comprises the off-diagonal elements of $\tilde{E}$ as follows:

$$\tilde{E}_1 = \tilde{E} - D_E, \tag{22}$$

and $\tilde{e}$ includes the sum of off-diagonal elements of each row as follows:

$$\tilde{e} = \tilde{E}_1 1_n. \tag{23}$$

Let $\tilde{F}$denotes the weighted line graph adjacancey without self loops then accordingly

$$\tilde{F} = \tilde{E}_1 + D_E^{1/2} \mathrm{diag}(\tilde{e})^{-1/2} \tilde{E}_1 \mathrm{diag}(\tilde{e})^{-1/2} D_E^{1/2} \tag{24}$$

Note that $\tilde{e}$ a characteristics of transmission lines, and $\tilde{F}$ is the equivalent for G' of $\tilde{A}$ for $\tilde{G}$. From this point onwards, the Line-Graph Based Model (LGBM) is represented by the weighted adjacency in (24). The description represents of the power grid in terms of G is referred to as a Bus-Based Model (BBM), while the description in terms on the line graph G' is referred to as a Line-Graph Based Model (LGBM) [35].For the weighted LGBM we denoted as $\tilde{G}'$.

III. COMPUTING GRAPH THEORTIC METRICS FOR BBM AND LGBM

It should be noted that our evaluation of robustness metrics for the power system has been based on static conditions. In the simulation of failures, the time-aspect cannot be taken into account. For example, nodes or links have only two states: functioning or non-functioning, and if a node or link is removed, as no new nodes / links are added, it remains removed. Robustness is therefore determined by the number of nodes or links removed.

Although the effect of flows through the network were beyond the scope of this study, future research could investigate the effects of flows. For example, for networks with limited power flow capacity, the consequences of a sole failure could be disastrous. Additionally, when a link or node is removed, power flow is redirected to alternative routes; redirection could cause overloading and the breakdown of other nodes or links. These failures could cause an increase in power flow and possibly generate other insecure events or even cascading failures.

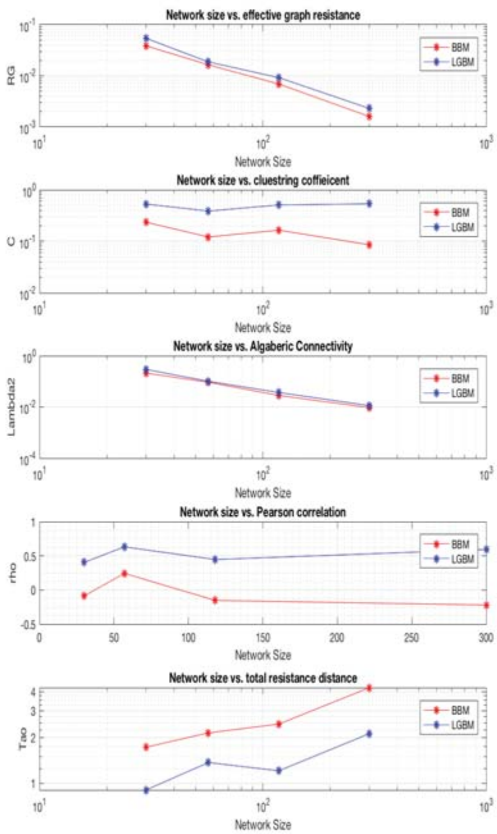

Fig. 1. Robustness metrics for IEEE test cases BBM and LGBM.

In our analysis of robustness measurements, we considered IEEE test cases of 30, 57, 118 and 300 buses. Fig. 1 visualize the robustness of BBM and LGBM vs. the size . Note that BBM shows better robustness comparing than LGBM , it means removing transmission is worse than removing buses.

IV. PREDICT RESILIANCE OF BBM AND LGBM BASED ON SFRE

A. Definition of SFRE

One of metrics that measure the resilience of the network is Sum of Flow Robustness based on Degree centrality (SFRD), which presented in [12], quantifies the reliable flows remaining after the attack. with Sum of Flow Robustness as illustrated in the Fig. 2. In this paper we use Eigenvalue centrality, in which the node with highest centrality is removed. The eigenvector centrality attack targets the node through which is the highest influence in the network. If the attack requires removing multiple nodes, centrality metrics are recomputed upon attacking each node. Sum of Flow Robustness based on Eigenvalue centrality (SFRE) captures resilience of a given network against eigenvalue -based attack.

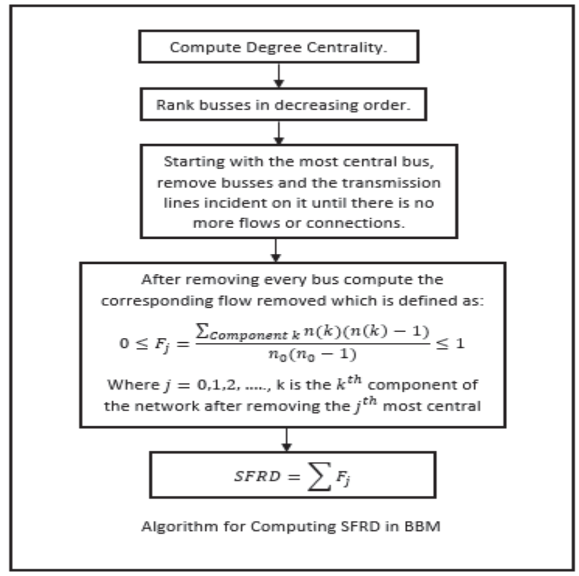

Fig. 2. Algorithm for Computing SFRD in BBM.

B. Prediction Resilience using SFRD and SFRE

We applied linear regression to calculate the precision of each graph's prediction of the power system's resilience. The Pearson correlation coefficient (ρ) indicates the extent to which there is linear correlation between two variables. If ρ is equal to 1 there is a perfect direct correlation, if it is -1, there is a perfect inverse correlation, and this value tends to 0 when no linear correlation is evident[27][29][30]. The original network (BBM) and the line-graph based network (LGBM) were analyzed using the measurements presented in Section III. Additionally, the sum of flow robustness towards degree attack (SFRD) and the sum of flow robustness towards eigenvalue attack (SFRE) estimated graph resilience to node attack. When ρ was used as a measure of accuracy to for the predictions of resilience measures SFRD and SFRE, it became evident that the number of average path length l for BBM had the highest values of accuracy overall (ρ(L,SFRD)=0.999 and (ρ(L,SFRE)=0.997. This metric retained high values for LGBM ρ(L,SFRD)=0.9845 and ρ(L,SFRE)=0.9928), however, the LGBM radius R demonstrated the highest correlations ρ(R,SFRD)=0.9893 and ρ(R,SFRE)=0.9931. Considering BBM, the diameter D was the second most predictive of SFRD and SFRE (ρ=0.9980, and ρ=0.9870, respectively). The LGBM also demonstrated high correlations with SFRD and SFRE (ρ=0.9845 and ρ=0.9928, respectively). Additionally, it is noted that As for LGBM had the lowest correlation with SFRD and SFRE ρ =0.36, and ρ=0.38, respectively), and for BBM, that the variance evident in the average degree metric $< k >$, indicates low accuracy. Furthermore, results demonstrated strong, inverse correlations for both effective graph resistance R and algebraic connectivity λ_2 with (ρ(X, SFRD) and (ρ(X, SFRE). In addition to accuracy metrics, network criticality placed second highest in the ranking of resilience measures (BBM = 0.97; LGBM = 0.87), as illustrated in in Tables II and III respectively.

TABLE I
RANKING OF BEST PREDICTORS METRICS OF RESILIENCE IN UNWEIGHTED NETWORKS

Ranking	BBM		LGBM	
	SFRD	SFRE	SFRD	SFRE
1	l	l	D,R	L
2	D	D	$\bar{l}$	D,$\bar{R}$
3	$\bar{R}$	L	L	$\bar{l}$
4	L	$\bar{R}$	τ	τ
5	τ	τ	R	R
6	λ_2	λ_2	λ_2	λ_2
7	R	R	$< k >$	$< k >$
8	CC	CC	CC	CC

TABLE II
ROBUSTNESS AND RESILIENCE PREDICTION OF BBM

BBM	30	57	118	300	$\rho(X, SFRD)$	$\rho(X, SFRE)$
N	30	57	118	300	-	-
L	41	78	179	409	0.9796	0.9737
$\bar{l}$	3.30	5.09	6.58	10.07	0.9991	0.9970
D	6	12	14	24	0.9980	0.9870
$\bar{R}$	4	7	7	13	0.9829	0.9585
R	0.0386	0.0164	0.0069	0.0016	-0.8911	-0.9143
τ	1.7274	2.1421	2.4492	4.2404	0.9777	0.9581
CC	0.235	0.122	0.165	0.086	-0.8509	-0.8201
λ_2	0.2121	0.0924	0.0282	0.0094	-0.8763	-0.9053
$< k >$	2.73	2.74	3.03	2.73	0.0399	0.1418
As	-0.0868	0.2432	-0.1526	-0.2206	-0.4833	-0.5246
$SFRD$	2.7402	5.6629	7.4200	12.6735	1	0.9946
$SFRE$	2.7264	11.4073	19.9577	33.8348	0.9946	1

TABLE III
ROBUSTNESS AND RESILIENCE PREDICTION OF LGBM

$LGBM$	30	57	118	300	$\rho(X, SFRD)$	$\rho(X, SFRE)$
N	41	78	179	409	-	-
L	100	170	509	1062	0.9792	0.9981
$\bar{l}$	3.063	4.630	6.040	9.360	0.9845	0.9928
D	7	11	15	23	0.9893	0.9931
$\bar{R}$	4	6	8	12	0.9893	0.9931
R	0.0540	0.0187	0.0092	0.0023	-0.8636	-0.7997
τ	0.9040	1.3687	1.2090	2.1206	0.8665	0.9085
CC	0.530	0.389	0.509	0.538	0.3943	0.4400
λ_2	0.2937	0.1014	0.0367	0.0113	-0.8605	-0.7910
$< k >$	4.88	4.36	5.69	5.19	0.5737	0.5026
As	0.4045	0.6323	0.4466	0.5937	0.3597	0.3797
$SFRD$	6.210	16.599	37.518	57.704	1	0.9876
$SFRE$	9.818	20.422	46.161	88.657	0.9876	1

Where :

N	Number of Nodes	τ	Network criticality
L	Number of Lines	CC	Clustering coefficient
$\bar{l}$	Average shortest path length	R	Effective graph resistance
D	Diameter	λ_2	Algebraic connectivity
$\bar{R}$	Radius	$< k >$	Degree

For a complete description see the Appendix

V. TO PREDICT RESILIANCE OF BBM AND LGBM BASED ON ELECTRICAL WEIGHTED NETWORKS

A. Weighted networks Prediction Resilience using SFRD and SFRE

In this section we reproduce section IV using weighted network in $\tilde{G}$ and $\tilde{G}'$. When ρ was used as a measure of accuracy to for the predictions of resilience measures SFRD and SFRE, it became evident that the number of CC for weighted BBM had the highest values of accuracy overall $\rho(CC$,SFRD)=0.995 and $\rho(CC$,SFRE)=0.995. This metric retained the lowest values for weighted LGBM ($\rho(CC$,SFRD)=0.6380 and $\rho(CC$,SFRE)=0.6896) because of the shared buses in LGBM, however, average path length $\bar{l}$ demonstrated the highest correlations $\rho(\bar{l}$,SFRD)= 0.9988 and $\rho(\bar{l}$,SFRE)=0. 0.9998. Considering BBM, the average path length $\bar{l}$ was the second most predictive of SFRD and SFRE (ρ=0.9724, and ρ=0.9761, respectively). The LGBM demonstrated average node degree $< K >$ as second high correlations with SFRD and SFRE (ρ=0.9905and ρ=0.9975, respectively). Additionally, it is noted that Network criticality τ for BBM had the lowest correlation with SFRD and SFRE (ρ =0.9608, and ρ=0.9652, respectively), as illustrated in in Tables V and VI respectively.

TABLE IV
RANKING OF BEST PREDICTORS METRICS OF RESILIENCE IN WEIGHTED NETWORKS

Ranking	BBM		LGBM	
	SFRD	SFRE	SFRD	SFRE
1	CC	CC	l	l
2	λ_2	$\bar{l}$	$< k >$	$< k >$
3	$\bar{l}$	$< k >$	λ_2	τ
4	$< k >$	λ_2	τ	λ_2
5	R,τ	R	R	R
6		τ	CC	CC

TABLE V
RANKING OF BEST PREDICTORS METRICS OF RESILIENCE WEIGHTED NETWORK

BBM	30	57	300	$\rho(X, SFRD)$	$\rho(X, SFRE)$
N	30	57	300	-	-
$\bar{l}$	38.195	83.0468	773.157	0.9724	0.9761
R	0.163	0.0748	1.79E-14	-0.9608	-0.9561
τ	0.4091	0.4688	6.208	0.9608	0.9652
CC	0.0682	0.0592	0.0343	-0.9995	-0.9999
λ_2	0.6714	0.3468	-2.17E-14	-0.9771	-0.9734
$< k >$	20.53	25.8213	117.49	0.971	0.9748
$SFRD$	2.74	5.66	12.673	1	0.9999
$SFRE$	2.73	11.4	33.835	0.9999	1

TABLE VI
ROBUSTNESS AND RESILIENCE PREDICTION OF WEIGHTED LGBM

$LGBM$	30	57	300	$\rho(X, SFRD)$	$\rho(X, SFRE)$
N	41	78	409	-	-
$\bar{l}$	10.0474	26.9553	120.169	0.9988	0.9998
R	0.1016	0.0478	0.0012	-0.9312	-0.9044
τ	0.4804	0.5235	3.9318	0.9836	0.9936
CC	0.2987	0.25	0.3259	0.6389	0.6896
λ_2	0.4364	0.2925	0.0021	-0.9903	-0.9786
$< k >$	26.9302	33.796	140.4022	0.9905	0.9975
$SFRD$	6.21	16.6	57.7	1	0.9977
$SFRE$	9.82	20.42	88.66	0.9977	1

VI. CONCLUSIONS

In this paper, robustness of the BBM network and the corresponding LGBM is addressed in relation to transmission line vulnerability. Some of the indicators described for network robustness include: network criticality, effective graph resistance, nodal degree distribution, flow robustness and algebraic connectivity.

This static model of the power grid was employed considering the similarity between the admittance matrix of the system and the Laplacian matrix of the corresponding graph. This relationship was then used for further analysis related to transmission line vulnerability, where we apply it to the weighted network in BBM and LGBM.

Robustness metrics were also used to measure the accuracy of the BBM and LGM models. This enabled the prediction of network resilience against targeted attacks on both a representation of the model of the current power network system, BBM, and of a theoretical LGBM. The sum of robustness flow for degree-based attacks and eigenvalue based attacks were employed as resilience measures.

Average path length, diameter, radius, network criticality, and effective graph resistance demonstrated good precision for the prediction of network resilience using the BBM graphs. Furthermore, for high precision in predicting the resilience of the LGBM network, average path length, diameter, and network criticality appear to be worthwhile estimates. LGBM is considered the most valuable contribution of this research where it evaluates the Robustness and Resilience Prediction Accuracy of transmission lines in the power system.

For the weighted networks clustering coefficient demonstrated good precision for the prediction of network resilience using the BBM weighted networks, and for average path length was for high precision in predicting the resilience of the LGBM weighted network .

Appendix

Shortest path (d) Path with least number of links or least total weights between nodes i and j in G [28]. We define shortest path (d) in terms of power system networks with the the path with leaset number of tranmssion lines between buses i and j in BBM.

Average shortest path length ($\bar{l}$) The average value of the shortest path across all possible pairs of buses on the graph [28].

Eccentricity(ε) The largest of the shortest distances between a specific bus v and other nodes on the graph [32].

Radius ($\bar{R}$) Represents the shortest eccentricity among nodes on the graph [32].

Graph diameter (D) Largest eccentricity among graph nodes [32].

Clustering coefficient (CC) Calculates the extent to which a bus neighbors are connected in BBM [28].

Degree Number of transmission lines connected to a bus i [32].

Fiedler eigenvalue or algebraic connectivity (λ_2) The Fiedler Eigenvalue of a graph G is defined as the second shortest eigenvalue of the Laplacian matrix [13]. Assuming that 0=$\lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_m$ are the eigenvalues of the Laplacian matrix ordered from smallest to largest, then λ_2 is the Fiedler eigenvalue.

To find the Laplacian matrix K we use the following expression :

$$\mathrm{K} = D - A, \tag{25}$$

where A is the adjacency matrix of G in (10), and D is the degree matrix in (12).

The pseudoinverse $K^\dagger$ of K is the matrix for which $x = K^\dagger K x$ for all x in the row space of K . The nullspace of $K^\dagger$ is the nullspace of K^T .

For the corresponding LGBM we use the following expression :

$$\tilde{\mathrm{K}} = D^L - A^L, \tag{26}$$

where A^L is the adjacency matrix of the line-graph network (G') in (13),D^L is the line-graph based model degree matrix.

A property of $\lambda_2(\tilde{\mathrm{K}})$ is that it is zero if the graph is not connected. If G is a connected graph, the algebraic connectivity will be above zero, also, its value will be upper-bounded by $m/(m-1)$ times the minimal nodal degree of the graph. The magnitude of this metric indicates the extent to which the overall graph is linked. If the Fiedler eigenvalue $\lambda_2(\tilde{\mathrm{K}})$ is near zero, network detachment is imminent [14] .

Network criticality (τ) Network criticality is a measurement of network robustness to topological changes [23]. As the criticality value decreases, network robustness increases.

$$\tau_G = \frac{2}{m-1}\mathrm{Trace}(K^\dagger), \tag{27}$$

where m is the size (number of nodes) of G and $(K^\dagger)$ is the pseudoinverse of of G Laplacian matrix [12].The expression (27) of the network criticality applied to G can be translated to G' as the following:

$$\tau_{G'} = \frac{2}{n-1}\mathrm{Trace}(\tilde{K}^\dagger), \tag{28}$$

where the superscript $G^{'}$ refers to the line graph, n is the size (number of nodes in LGBM) of $G^{'}$ and $(\tilde{K}^\dagger)$ is the pseudoinverse of Laplacian matrix for $G^{'}$.

Effective graph resistance (R) The effective resistance of a graph, referred as R, is a metric related to a graph G that also provides information on network strength when it is subject to the removal of nodes or links. The greater the effective resistant, the more robust the network [24]. R_G in G is determined using the following :

$$R_G = m \sum_{i=2}^{m} \frac{1}{\lambda_i}, \tag{29}$$

which utilizes the Laplacian matrix eigenvalues.

The corresponding effective graph resistance $R_{G'}$ for the LGBM is determined using (30).

$$R_{G'} = n \sum_{i=2}^{n} \frac{1}{\tilde{\lambda}_i}. \tag{30}$$

Flow robustness ($\hat{\text{F}}$) According to [12], robustness to flow on a graph $\hat{F}_G$, indicates the proportion of unfailing flows to the total amount of flows in the system. Flow robustness values range from zero to one, where one indicates that all nodes are able to communicate, and zero, that there is no communication. It is said that a flow is unfailing or reliable if even one of its connection pathways survives. For LGBM, total combined flows is the most extreme amount of flows $n(n-1)/2$ for n transmission line .

Flow robustness utilizes the capacity of nodes in the network to interconnect. It can be computed using the following :

$$\hat{F}_G = \frac{\sum_{i=1}^{k} \xi_i(\xi_i - 1)}{m(m-1)}, \tag{31}$$

where ξ_i is the set of components in graph G . For LGBM it can be computed using:

$$\hat{F}_{G'} = \frac{\sum_{i=1}^{k} \xi_i^L(\xi_i^L - 1)}{n(n-1)}, \tag{32}$$

where ξ^L represents the number of components in G'.

References

[1] L. Mili and Q. Qiu, “Risk assessment of catastrophic failures in electric power systems,” Int. J. Crit. Infrastructures, vol. 1, no. 1, pp. 38–63, 2004.

[2] M. M. Rosas-Casals, S. Valverde, and R. V. Solé, “Topological Vulnerability of the European Power Grid Under Errors and Attacks,” Int. J. Bifurc. Chaos, vol. 17, no. 7, pp. 2465–2475, 2007.

[3] B. A. Carreras and V. E. Lynch, “Critical points and transitions in an electric power transmission model for cascading failure blackouts,” vol. 12, no. 4, 2002.

[4] G. A. Pagani and M. Aiello, “The Power Grid as a complex network: A survey,” Phys. A Stat. Mech. its Appl., vol. 392, no. 11, pp. 2688–2700, 2013.

[5] Y. Koç, M. Warnier, R. E. Kooij, and F. M. T. Brazier, “Structural vulnerability assessment of electric power grids,” Proc. 11th IEEE Int. Conf. Networking, Sens. Control, no. August 2016, pp. 386–391, 2014.

[6] G. Zhao Yang Dong, J. Junhua Zhao, S. R. Weller, and S. R. Guo Chen, “Complex Network Theory based Power Grid Vulnerability Assessment from Past to Future,” 9th IET Int. Conf. Adv. Power Syst. Control. Oper. Manag. (APSCOM 2012), no. November, pp. 162–162, 2012.

[7] Diestel, R. 2006. Graph Theory, 3rd Ed. Springer-Verlag, Berlin.

[8] Å.˚ J. Holmgren, “Using graph models to analyze the vulnerability of electric power networks,” Risk Anal., vol. 26, no. 4, pp. 955–969, 2006.

[9] D. J. Watts and S. H. , “Collective dynamics of small-world networks,” Nature, vol. 393, no. 6684, pp. 440–442, 1998.

[10] T. A. Ernster and A. K. , “Power system vulnerability analysis - Towards validation of centrality measures,” Proc. IEEE Power Eng. Soc. Transm. Distrib. Conf., pp. 1–6, 2012.

[11] Z. Wang, A. , and R. J. Thomas, “Electrical centrality measures for electric power grid vulnerability analysis,” Proc. IEEE Conf. Decis. Control, pp. 5792–5797, 2010.

[12] M. J. F. Alenazi and J. P. G. , “Comprehensive comparison and accuracy of graph metrics in predicting network resilience,” 2015 11th Int. Conf. Des. Reliab. Commun. Networks, DRCN 2015, pp. 157–164, 2015.

[13] M. Fiedler, “Algebraic connectivity of graphs,” Czechoslov. Math. J., vol. 23, no. 2, pp. 298–305, 1973.

[14] A. Jamakovic and S. Uhlig, “Influence of the network structure on robustness,” 2007 15th IEEE Int. Conf. Networks, pp. 278–283, 2007.

[15] L. Cuadra, S. Salcedo-Sanz, J. Del Ser, S. - Fernández, and Z. W. Geem, “A critical review of robustness in power grids using complex networks concepts,” Energies, vol. 8, no. 9, pp. 9211–9265, 2015.

[16] C. J. Kim and O. B. Obah, “Vulnerability assessment of power grid using graph topological indices,” Int. J. Emerg. Electr. Power Syst., vol. 8, no. 6, 2007.

[17] Ke Sun, “Complex Networks Theory: A New Method of Research in Power Grid,” 2005 IEEE/PES Transm. Distrib. Conf. Expo. Asia Pacific, pp. 1–6, 2005.

[18] P. Chopade and M. , “Critical infrastructure interdependency modeling: Using graph models to assess the vulnerability of smart power grid and SCADA networks,” 2011 8th Int. Conf. Expo Emerg. Technol. a Smarter World, CEWIT 2011, pp. 1–6, 2011.

[19] A. von Meier, Electric Power Systems: A Conceptual Introduction. Wiley, 2006.

[20] T. Yoshida, “Weighted line graphs for overlapping community discovery,” Soc. Netw. Anal. Min., vol. 3, no. 4, pp. 1001–1013, 2013.

[21] N. Suri and G. Cabri, Adaptive, Dynamic, and Resilient Systems. Taylor & Francis, 2014.

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

[23] A. Tizghadam and A. Leon-garcia, “Autonomic Traffic Engineering for Network Robustness,” vol. 28, no. 1, pp. 1–12, 2010.

[24] X. Wang, E. Pournaras, R. E. Kooij, and P. Van Mieghem, “Improving Robustness of Complex Networks via the Effective Graph Resistance,” pp. 1–12, 2014.

[25] Z. Wang, A. , and R. J. Thomas, “Generating statistically correct random topologies for testing smart grid communication and control networks,” IEEE Trans. Smart Grid, vol. 1, no. 1, pp. 28–39, 2010.

[26] E. Castillo and A. S. Hadi, “Fitting the Generalized Pareto Distribution to Data,” J. Am. Stat. Assoc., vol. 92, no. 440, pp. 1609–1620, 1997.

[27] G. L. Shevlyakov and H. Oja, Robust Correlation: Theory and Applications. Wiley, 2016.

[28] Pastor-Satorras, R., and Alessandro Vespignani. 2004. Evolution and Structure of the Internet : A Statistical Physics Approach. Cambridge, UK: Cambridge University Press, 2004.

[29] O. T. Daniel and M. Bikdash, "Simulating the effect of soft undulating surface on outdoor noise propagation using equivalent sources," SoutheastCon 2015, Fort Lauderdale, FL, 2015, pp. 1-8. doi: 10.1109/SECON.2015.7133014

[30] Yogesh S. Kale, Xiangfeng Dai, Bradley Meyer, Samantha E. Petrie, Marwan Bikdash, and Michael D. Topal. 2017. An Extensible Recommendation System for Health Research. In Proceedings of the SouthEast Conference (ACM SE ’17). ACM, New York, NY, USA, 95-101. DOI: https://doi.org/10.1145/3077286.3077296

[31] Norbert A. Agana, Abdollah Homaifar, ”A Deep Learning Base Approach for Long-Term Drought Forecasting”, IEEE SoutheastCon, March 30 - April 2, 2017, Charlotte, NC, USA

[32] Dehmer, Matthias. 2011. Structural Analysis of Complex Networks. Boston, Mass.: Birkhäuser,2011.

[33] P. and M. Bikdash, “Modeling for survivability of Smart Power Grid when subject to severe emergencies and vulnerability” 2012 Proceedings of IEEE Southeastcon,2012.

[34] P. Chopade and M. Bikdash, “Analyzing Smart Power Grid and SCADA network robustness using the node degree distribution and algebraic connectivity under vulnerability and WMD attacks” 2012 IEEE conf. on technologies for homeland security (HST), 2012

[35] A. Albarakati , M. Bikdash, and X. Dai, “Line-Graph Based Modeling for Assessing the Vulnerability of Transmission Lines” 2017 Proceedings of IEEE Southeastcon, 2017.

[36] A. Meier, Electric Power System-A Conceptual Introduction, IEEE Press, A John Wiley & Sons, Inc., Publications, 2006.

[37] L. Grigsby, Electric Power Engineering Handbook, Second Edition, CRC Press, 2006.