Assessing and Safeguarding Network Resilience to Nodal Attacks

Pin-Yu Chen and Alfred O. Hero III, *Fellow*, *IEEE*
Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, USA
Email : {pinyu,hero}@umich.edu

***Abstract*—This paper introduces new methods for evaluating and improving resilience of network connectivity to attacks or failures on nodes of the network. The network connectivity is evaluated using a new centrality measure that quantifies sensitivity of the size of the largest connected component to node removals. Based on this centrality measure, a new method for improving resilience is introduced called *edge rewiring*. The topology of the power grid of western US states is used to illustrate the proposed methods. Using the proposed centrality measure, we show that the power grid topology is especially vulnerable to nodal attacks. In particular, by using our new centrality measure, an attacker could reduce the largest component size by nearly a factor of two by only targeting 0.2% of the nodes. More importantly, we show that network resilience can be greatly improved via a few edge rewires without introducing additional edges in the network.**

***Index Terms*—centrality attacks, edge addition, edge rewiring, network connectivity**

I. Introduction

The problem of establishing resilience of network connectivity to node removals has received much recent attention [1]–[4]. Resilience is closely related to reliability of networks when a subset of nodes are inactivated. This problem arises in applications including service disruption in communication systems caused by terminal failures, and blackout in power systems caused by power station shutdowns, among others. In these applications network functionality can be disrupted by targeted attacks, e.g., Denial of service (DoS) or jamming attacks, or by natural occurrences, e.g., weather-related link failures and power outages. In this paper we introduce a new method for assessing the resilience of networks to node removals and preventive approaches to connectivity attacks.

A resilient network has global connectivity and largest component size that are only minimally disrupted by limited attacks on nodes or edges. For example, a fully connected network allows communication between all pairs of nodes and its largest component is the entire set of nodes in the network. One measure of network connectivity is given by the standard graph-theoretic definition: for a fully connected graph connectivity is the minimum number of node removals required to reduce the size of the largest component. However, this definition does not account for the number of communication paths between nodes that are disrupted, which is more relevant to the functioning of the network. A more relevant measure of connectivity is proposed here: the minimum number of node removals necessary to reduce the size of the largest component by a fixed proportion, e.g. 10% or 50%, of its original size.

To illustrate consider a large network where one of its nodes is connected to the rest of the network by a single edge (i.e., node degree one). Removing this edge (or the adjacent node) will reduce both the number of communication paths and the largest component size by one. However, if the network is composed of two cliques of equal size connected by a single edge then removal of this edge will reduce the number of paths and the largest component size by a factor of two.

A node centrality measure is a quantity that measures the level of importance of a node in a network. The utility of centrality measures is that they can break the combinatorial bottleneck of searching through all the possible permutations and combinations of nodes that might reduce largest component size. An attack that removes nodes according to a measure of centrality, such as the one introduced in Sec. II, will be referred to a *centrality attack*. For example, the authors of [1], [2] and [3] study the effectiveness of degree centrality attacks, i.e., removing the largest hub nodes, as a way to reduce the size of the largest component of the network. However, it has been shown in [4] that node degree is not the most effective centrality measure for minimizing largest component size. For different network topologies, investigating resilience of network connectivity to centrality attacks provides a unified metric for evaluating network vulnerabilities.

Quantitative network resilience measures can be used to assess the effectiveness of preventive approaches for hardening a network against attacks. Two preventive approaches are discussed in this paper. The first method is the *edge addition* method [5], where edges are added to the network to enhance network resilience. The second method is the proposed *edge rewiring* method, where new edges are introduced by swapping a subset of existing edges.

One possible advantage of the edge rewiring method is that it requires no additional edges to enhance network resilience. The edge rewiring method might be preferable to the edge addition method in the following aspects:

- **Lower operational and maintenance costs**: for power grids, power dissipation and facility maintenance costs are proportional to the total number of edges in the network.
- **Easier link monitoring for network security**: in large-scale systems such as Internet and cellular infrastructures, introducing additional edges inevitably raises the security risks to information exposure, and it also incurs extra burden for system administration and monitoring.
- **Reduced provisioning budget**: in networking paradigms

TABLE I
SUMMARY OF CENTRALITY MEASURES

	Global measure	Local measure	Mathematical expression
Betweenness	✓		$\text{betweenness}(i) = \sum_{k\neq i}\sum_{j\neq i, j>k} \frac{\sigma_{kj}(i)}{\sigma_{kj}}$
Closeness	✓		$\text{closeness}(i) = 1/\sum_{j\in\mathcal{V}, j\neq i} \rho(i,j)$
Eigenvector centrality (eigen centrality)	✓		$\text{eigen}(i) = \lambda_{\max}^{-1}\sum_{j\in\mathcal{V}} \mathbf{A}_{ij}\xi_j$
Degree		✓	$d_i = \sum_{j\in\mathcal{N}_i} \mathbf{A}_{ij}$
Ego centrality		✓	$\text{ego}(i) = \sum_k \sum_{j>k} 1/\left[\mathbf{A}^2(i) \circ (\mathbf{I} - \mathbf{A}(i))\right]_{kj}$
Local Fiedler Vector Centrality (LFVC)	✓[1]		$\text{LFVC}(i) = \sum_{j\in\mathcal{N}_i}(y_i - y_j)^2$

with stringent energy/bandwidth constraints such as sensor networks and peer-to-peer (P2P) networks, establishing additional edges consumes more networking resources.

To illustrate resilience of network connectivity to different centrality attacks and effectiveness of preventive approaches we consider the power grid network for western US states [7]. We show that different centrality measures differ significantly in their ability to assess resilience of this real-world network. If the proposed centrality measure is used by an attacker, the largest component size can be reduced to nearly half of its original size by removing only 0.2% of nodes in the network. Attacks using other types of centrality measures are less effective in reducing largest component size. In particular, even if as many as 1% of the nodes are removed, less than 6% reduction in largest component size is achieved by other types of centrality attacks. In addition, we show that the proposed edge rewiring method can greatly improve network resilience via only a few edge rewires while achieving the same performance as the edge addition method.

The rest of the paper is organized as follows. Sec. II reviews several centrality measures, and their properties are summarized in Table I. Sec. III investigates the resilience of network connectivity to different centrality attacks on the power grid topology. Sec. IV discusses the edge addition method and the proposed edge rewiring method as preventive approaches to centrality attacks. We implement the two preventive approaches and evaluate their performances on the power grid topology in Sec. V. Finally, Sec. VI concludes the paper. For notations, uppercase letters in boldface represent matrices, lowercase letters in boldface represent vectors, and uppercase letters in calligraphic face represent sets. $(\cdot)^T$ denote matrix and vector transpose.

II. CENTRALITY MEASURES

Consider a network as a connected graph $G = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the set of nodes and $\mathcal{E}$ is the set of edges. The connectivity structure of G can be represented by the $|\mathcal{V}| \times |\mathcal{V}|$ adjacency matrix $\mathbf{A}$, where $|\mathcal{V}|$ is the number of nodes in G and $\mathbf{A}_{ij} = 1$ if node i and node j are connected by an edge, otherwise $\mathbf{A}_{ij} = 0$. Let $\mathcal{N}_i$ denote the set of nodes connecting to node i (i.e., the set of neighbors of node i), the degree of a node is the number of edges connected to it, i.e., $d_i = \sum_{j\in\mathcal{N}_i} \mathbf{A}_{ij}$. The degree matrix $\mathbf{D}$ is defined as $\mathbf{D} = \text{diag}\left(d_1, d_2, \ldots, d_{|\mathcal{V}|}\right)$, where $\mathbf{D}$ is a diagonal matrix with degree information on its main diagonal and the rest of the entries being 0. The graph Laplacian matrix $\mathbf{L}$ is defined as $\mathbf{L} = \mathbf{D} - \mathbf{A}$, and therefore it encodes degree information and connectivity structure of a graph. $\mathbf{L}$ is a positive semidefinite matrix that all its eigenvalues are nonnegative and $\text{trace}(\mathbf{L}) = 2|\mathcal{E}|$, where $\text{trace}(\mathbf{L})$ is the sum of eigenvalues of $\mathbf{L}$ and $|\mathcal{E}|$ is the number of edges in G. Moreover, the smallest eigenvalue of $\mathbf{L}$ is always 0 and the eigenvector of the smallest eigenvalue is a constant vector. The second smallest eigenvalue of $\mathbf{L}$, denoted by $\mu(\mathbf{L})$, is also known as the algebraic connectivity [8]. It has been proved in [8] that $\mu(\mathbf{L})$ is a lower bound on node and edge connectivity for any non-complete graphs. That is, algebraic connectivity $\leq$ node connectivity $\leq$ edge connectivity.

Centrality measures can be classified into two categories, *global* and *local* measures. Global centrality measures require complete topological information for their computation, whereas local centrality measures only require partial topological information from neighboring nodes. For instance, acquiring shortest path information between every node pair is a global method, and acquiring degree information of every node is a local method. Some commonly used centrality measures are:

- **Betweenness** [9]: betweenness measures the fraction of shortest paths passing through a node relative to total shortest paths in the network. Specifically, betweenness is a global measure defined as $\text{betweenness}(i) = \sum_{k\neq i}\sum_{j\neq i, j>k} \frac{\sigma_{kj}(i)}{\sigma_{kj}}$, where σ_{kj} is the total number of shortest paths from k to j and $\sigma_{kj}(i)$ is the number of such shortest paths passing through i.
- **Closeness** [10]: closeness is a global measure of geodesic distance of a node to all other nodes. A node is said to have higher closeness if the sum of its shortest path distance to other nodes is smaller. Let $\rho(i,j)$ denote the shortest path distance between node i and node j in a connected graph. $\text{closeness}(i) = 1/\sum_{j\in\mathcal{V}, j\neq i} \rho(i,j)$.
- **Eigenvector centrality** (eigen centrality) [11]: eigenvector centrality is the ith entry of the eigenvector associated with the largest eigenvalue of the adjacency matrix $\mathbf{A}$. It is defined as $\text{eigen}(i) = \lambda_{\max}^{-1}\sum_{j\in\mathcal{V}} \mathbf{A}_{ij}\xi_j$, where $\lambda_{\max}$ is the largest eigenvalue of $\mathbf{A}$ and ξ is the eigenvector associated with $\lambda_{\max}$. It is a global measure since eigenvalue decomposition on $\mathbf{A}$ requires complete topological

[1] Although LFVC is a global centrality measure, it is locally computable via distributed power iteration method [6].

information.

- **Degree** (d_i): degree is the simplest local measure that accounts for the number of neighboring nodes.
- **Ego centrality** [12]: consider the $(d_i{+}1)$-by-$(d_i{+}1)$ local adjacency matrix of node i, denoted by $\mathbf{A}(i)$, and let $\mathbf{I}$ be an identity matrix. Ego centrality can be viewed as a local version of betweenness that computes the shortest paths between its neighboring nodes. Since $[\mathbf{A}^2(i)]_{kj}$ is the number of two-hop walks between k and j, and $\left[\mathbf{A}^2(i) \circ (\mathbf{I} - \mathbf{A}(i))\right]_{kj}$ is the total number of two-hop shortest paths between k and j for all $k \neq j$, where $\circ$ denotes entrywise matrix product, ego centrality is defined as $\text{ego}(i) = \sum_k \sum_{j>k} 1/\left[\mathbf{A}^2(i) \circ (\mathbf{I} - \mathbf{A}(i))\right]_{kj}$.
- **Local Fiedler Vector Centrality** (LFVC) [13]: LFVC is a new measure that characterizes vulnerability to node removals. A node with higher LFVC is more important for network connectivity structure. Let $\mathbf{y}$ (the Fiedler vector) denote the eigenvector associated with the second smallest eigenvalue $\mu(L)$ of the graph Laplacian matrix $\mathbf{L}$, LFVC is defined as $\text{LFVC}(i) = \sum_{j\in\mathcal{N}_i}(y_i - y_j)^2$. Although LFVC is a global centrality measure, it can be accurately approximated by local computations and message passing using the distributed power iteration method of [6] to compute the Fiedler vector $\mathbf{y}$.

The aforementioned centrality measures and their properties ties are summarized in Table I.

III. Resilience of Western US States Power Grid Topology to Centrality Attacks

Throughout this paper we adopt a greedy node removal strategy that sequentially removes the node with highest centrality measure from the remaining largest component. The centrality measure is recalculated after node removals. It has been shown in [14] that greedy node removal strategies can be effective reducers of the largest component size as compared with batch node removal strategies based on the same centrality measure. In general, there is no performance guarantee relating the greedy node removal strategy and the optimal batch removal strategy. However, using submodularity of the LFVC measure (i.e., diminishing gain on the upper bound of resulting algebraic connectivity when nodes with highest LFVC measures are sequentially removed), it is proved in [13] that greedy node removal based on LFVC comes within at least $1 - 1/e$ of the performance of an optimal batch node removal strategy, where e is the Euler's constant. Therefore one might expect that greedy LFVC attacks can severely impact network connectivity.

We use the topology of power grid of western US states [7] to illustrate the application of our centrality measure (LFVC) for assessing vulnerability to different types of centrality attacks. The results are shown in Fig. 1. This network contains 4941 nodes and 6594 edges, where nodes represent power stations and edges represent power lines. More network topology information can be found in the supplementary file. One can see from Fig. 1 that an LFVC attack is capable of reducing the largest component size to roughly 54% of its original size by removing only 8 nodes from the network. On the other hand, betweenness and closeness attacks require 28 and 31 node removals, respectively, to achieve the same performance. Equivalently, the LFVC attack requires only 0.2% of the nodes to be removed to severely disrupt the communications between nearly half of the nodes in the network. In addition, degree, eigen centrality, and ego centrality attacks fail to significantly disrupt the network (less than 6% reduction in largest component) even when 1% of the nodes are attacked. By inspecting the adjacency matrix $\mathbf{A}$ in [7], it is observed that the adjacency matrix has apparent blockwise structure where blocks are densely connected subgrids that are interconnected by relatively a few inter-subgrid edges. Since the high-degree nodes are not connected to the inter-subgrid edges and each subgrid is densely connected, greedy degree attacks do not result in severe connectivity loss. We conclude that LFVC attacks do significantly more damage than other types of centrality attacks. Therefore, LFVC is a more reliable measure of resilience of the network.

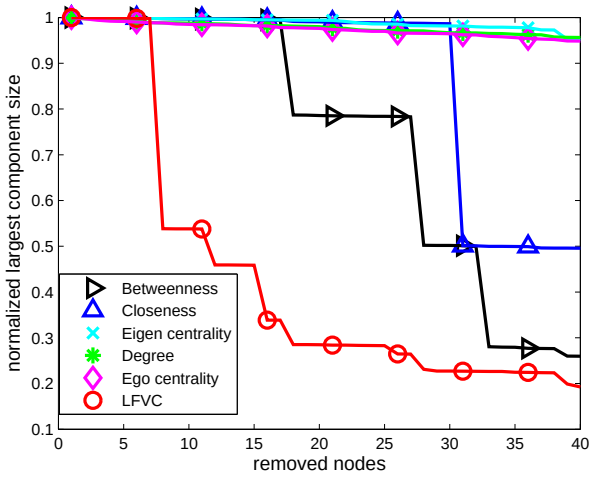

Fig. 1. Resilience of network connectivity to different centrality attacks on the power grid topology of western US states [7]. This network contains 4941 nodes and 6594 edges, where nodes represent power stations and edges represent power lines. By removing roughly 0.2% of the nodes in the network based on an LFVC attack, the largest component size is reduced to nearly half of its original size.

IV. Preventive Approaches to Centrality Attacks

Here we discuss two preventive approaches to protect against centrality attacks, namely the *edge addition* method and the *edge rewiring* method.

A. Edge addition method

Edge addition is perhaps the most intuitive method for enhancing resilience of network connectivity since it adds edges that are not already present in G. Let $\widehat{\mathbf{L}}$ be the resulting graph Laplacian matrix after adding an edge $(i,j) \notin \mathcal{E}$ to G and let $\mathbf{1}$ be a vector of all ones. Recalling the definition of the graph Laplacian matrix $\mathbf{L}$ in Sec. II, $\widehat{\mathbf{L}} - \mathbf{L} = (\mathbf{e}_i - \mathbf{e}_j)(\mathbf{e}_i - \mathbf{e}_j)^T$, where $\mathbf{e}_i$ is an all-zero vector except its ith entry being 1. The term $(\mathbf{e}_i - \mathbf{e}_j)(\mathbf{e}_i - \mathbf{e}_j)^T$ corresponds to the graph Laplacian

matrix of the removed edge (i, j). Since the algebraic connectivity $\mu(\mathbf{L})$ is the second smallest eigenvalue of $\mathbf{L}$ and the smallest eigenvalue of $\mathbf{L}$ is 0 with the associated eigenvector $\mathbf{1}$, we have the representation $\mu(\mathbf{L}) = \min_{\|\mathbf{x}\|_2=1, \mathbf{x}^T\mathbf{1}=0} \mathbf{x}^T\mathbf{L}\mathbf{x}$ [8]. It is proved in [5] that

$$\mu(\widehat{\mathbf{L}}) \geq \mu(\mathbf{L}) + c_1 \cdot (y_i - y_j)^2, \tag{1}$$

where $\mathbf{y}$ is the eigenvector of $\mu(\mathbf{L})$ and $c_1 > 0$ is a positive constant.

Since algebraic connectivity is a lower bound of node connectivity and edge connectivity, it is proposed in [5] that one should iteratively add an edge that maximizes the quantity $(y_i - y_j)^2$ to the graph. For each iteration, the edge that maximizes $(y_i - y_j)^2$ maximizes the lower bound on the resulting algebraic connectivity, and therefore enhances network resilience to centrality attacks. The edge addition method serves as the baseline performance comparison to the proposed edge rewiring method.

B. Edge rewiring method

Edge rewiring aims to rewire the edges in the graph to enhance the resilience of network connectivity to attacks. In particular, edge rewiring method does not change the total number of edges in the graph. The algorithm for the proposed edge rewiring method is summarized as follows.

Algorithm Edge rewiring method

Input: number of rewires r, graph $G = (\mathcal{V}, \mathcal{E})$
Output: rewired graph $\widetilde{G} = (\mathcal{V}, \widetilde{\mathcal{E}})$
for $i = 1$ to r **do**
  Compute the second smallest eigenvector $\mathbf{y}$ of $\mathbf{L}$
  Compute the largest eigenvector $\mathbf{z}$ of $\mathbf{L}$
  Find $(i^*, j^*) = \arg\max_{(i,j)\notin\mathcal{E}} (y_i - y_j)^2$
  Find $(k^*, \ell^*) = \arg\max_{(k,\ell)\in\mathcal{E}} (z_k - z_\ell)^2$
  Edge addition stage: $\widetilde{\mathcal{E}} \leftarrow \mathcal{E} \cup (i^*, j^*)$
  Edge deletion stage: $\widetilde{\mathcal{E}} \leftarrow \widetilde{\mathcal{E}} / (k^*, \ell^*)$
  $G \leftarrow \widetilde{G}$
end for

For each rewire, the edge rewiring method consists of two stages: an *edge addition* stage and an *edge deletion* stage. In the edge addition stage, similar to the edge addition method, an edge $(i, j) \notin \mathcal{E}$ that maximizes $(y_i - y_j)^2$ is selected to maximize the lower bound on the resulting algebraic connectivity in (1). Let $\phi(\mathbf{L})$ denote the largest eigenvalue of $\mathbf{L}$ and $\mathbf{z}$ denote the associated eigenvector of $\phi(\mathbf{L})$. In the edge deletion stage, an edge $(k, \ell) \in \mathcal{E}$ that maximizes $(z_k - z_\ell)^2$ is removed. The reason is explained as follows. Let $\widetilde{\mathbf{L}}$ denote the graph Laplacian matrix after removing an edge from G. Since $\text{trace}(\mathbf{L}) - \text{trace}(\widetilde{\mathbf{L}}) = 2$, i.e., 2 times the number of edge removals, and by Cauchy's eigenvalue interlacing property [15], $\phi(\mathbf{L}) \geq \phi(\widetilde{\mathbf{L}})$ and $\mu(\mathbf{L}) \geq \mu(\widetilde{\mathbf{L}})$, we have

$$\mu(\widetilde{\mathbf{L}}) \geq \mu(\mathbf{L}) + \phi(\mathbf{L}) - \phi(\widetilde{\mathbf{L}}) - 2. \tag{2}$$

Consequently, for maximum effect, the edge rewiring algorithm should remove the edge that maximizes $\phi(\mathbf{L}) - \phi(\widetilde{\mathbf{L}})$ such that the lower bound on the resulting algebraic connectivity in (2) is maximized. By definition, $\phi(\mathbf{L}) = \max_{\|\mathbf{x}\|_2=1} \mathbf{x}^T\mathbf{L}\mathbf{x}$, and $\mathbf{L} - \widetilde{\mathbf{L}} = (\mathbf{e}_k - \mathbf{e}_\ell)(\mathbf{e}_k - \mathbf{e}_\ell)^T$ when the edge $(k, \ell) \in \mathcal{E}$ is removed. Therefore, computing $\mathbf{z}^T\widetilde{\mathbf{L}}\mathbf{z}$, we have $\phi(\mathbf{L}) - \phi(\widetilde{\mathbf{L}}) \leq (z_k - z_\ell)^2$. Moreover, by the eigenvector property that $\mathbf{z}$ is orthogonal to $\mathbf{1}$ (i.e., $\mathbf{z}^T\mathbf{1} = 0$), it is easy to verify that there exists an edge $(k, \ell) \in \mathcal{E}$ and a constant $c_2 > 0$ such that $\phi(\mathbf{L}) - \phi(\widetilde{\mathbf{L}}) \geq c_2 \cdot (z_k - z_\ell)^2$.

Note that since the eigenvector $\mathbf{y}$ associated with $\mu(\mathbf{L})$ can be computed in a distributed manner [6], the eigenvector $\mathbf{z}$ associated with $\phi(\mathbf{L})$ can also be obtained using distributed local computations and message passing.

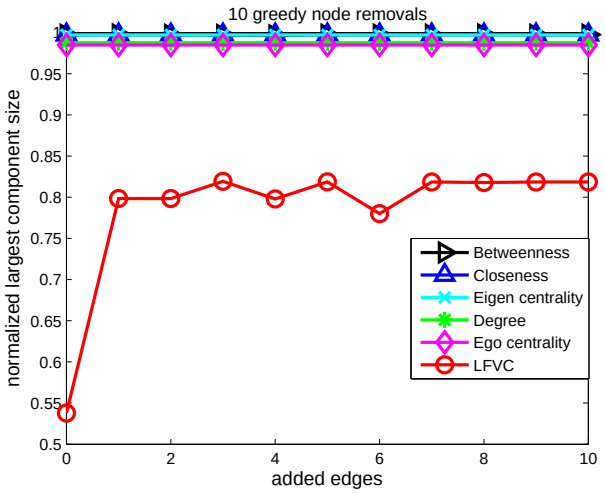

Fig. 2. Network connectivity of the edge addition method when restricted to 10 greedy node removals on the power grid topology of western US states [7]. The network connectivity can be enhanced from 54% to 80% under LFVC attacks by adding one edge.

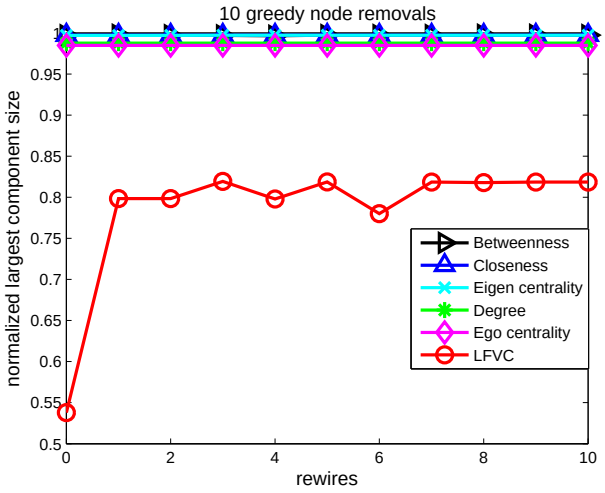

Fig. 3. Network connectivity of the edge rewiring method when restricted to 10 greedy node removals on the power grid topology of western US states [7]. The proposed edge rewiring method can perform as well as the edge addition method without introducing additional edges in the network.

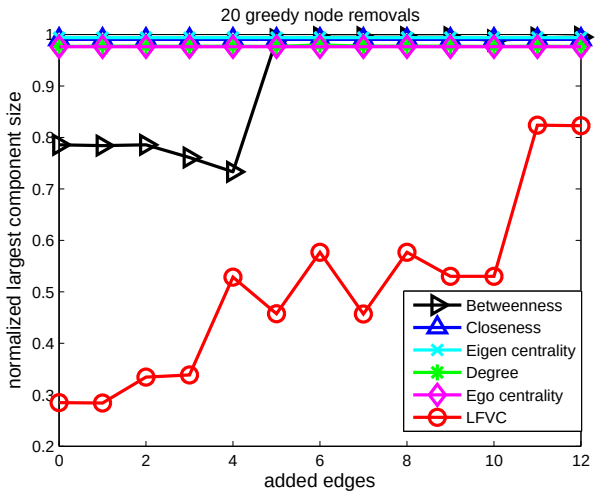

Fig. 4. Network connectivity of the edge addition method when restricted to 20 greedy node removals on the power grid topology of western US states [7]. 11 additional edges are required to enhance the network connectivity from 29% to 82%.

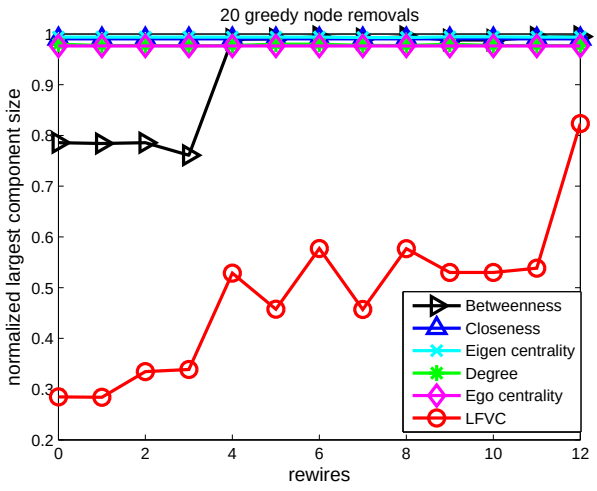

Fig. 5. Network connectivity of the edge rewiring method when restricted to 20 greedy node removals on the power grid topology of western US states [7]. The proposed edge rewiring method requires only 12 edge rewires to achieve the same performance as in Fig. 4, which means that we only need to rewire fewer than 0.4% of edges to make it resilient to centrality attacks.

V. Performance Evaluation

In this section, we evaluate the effectiveness of the edge addition and edge rewiring methods on protecting the power grid topology [7] from centrality attacks. When 10 nodes are removed from the network by LFVC attacks, Fig. 1 shows that the network connectivity is reduced to 54%. In contrast, under other types of centrality attacks there is almost no loss in connectivity when 10 nodes are removed. Fig. 2 illustrates the effect of edge addition as a preventive approach against centrality attacks. It is observed that by adding one edge, the network connectivity can be increased from 54% to 80% under LFVC attack. Fig. 3 illustrates the proposed edge rewiring method. Similar to the edge addition method, one edge rewire is capable of enhancing the network connectivity from 54% to 80%. Thus using the edge rewiring method with only one edge rewire can protect the network as well as the edge addition method even though the latter introduces additional edges in the network.

When 20 nodes are removed from the network, as shown in Fig. 4, 11 edge additions are required to enhance the network connectivity from 29% to 82%. In comparison, as shown in Fig. 5, the proposed edge rewiring method requires only 12 edge rewires to achieve the same performance, which means that we only need to rewire fewer than 0.4% of edges to make it resilient to centrality attacks. This performance advantage is explainable since, for the same number of edge adding or rewiring actions, edge rewiring changes twice as many edges in the network as edge addition. A second illustrative example for an European Internet backbone network is discussed in the supplementary file.

VI. Conclusion and Future Work

This paper investigates network resilience to centrality attacks, proposes a new centrality measure for assessing resilience, and studies two preventive approaches for protecting networks against such attacks. The results on the power grid of western US states show that the network is particularly vulnerable to LFVC attacks, and the edge rewiring method can significantly improve network resilience with only a few edge rewires. Useful areas for future work are: 1) extension to time-varying topologies; 2) extension to topologies with weighted edges; and 3) application to social networks.

Acknowledgement

This work has been partially supported by the Army Research Office (ARO), grant number W911NF-12-1-0443.

References

[1] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, July 2000.
[2] S. Xiao, G. Xiao, and T. H. Cheng, "Tolerance of intentional attacks in complex communication networks," *IEEE Commun. Mag.*, vol. 45, no. 1, pp. 146–152, Feb. 2008.
[3] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen, "Smart attacks in smart grid communication networks," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 24–29, Aug. 2012.
[4] P.-Y. Chen and A. Hero, "Node removal vulnerability of the largest component of a network," in *Proc. IEEE GlobalSIP*, 2013.
[5] A. Ghosh and S. Boyd, "Growing well-connected graphs," in *Proc. IEEE Conference on Decision and Control*, 2006, pp. 6605–6611.
[6] A. Bertrand and M. Moonen, "Distributed computation of the Fiedler vector with application to topology inference in ad hoc networks," *Signal Processing*, vol. 93, no. 5, pp. 1106–1117, 2013.
[7] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, no. 6684, pp. 440–442, June 1998. [Online]. Available: http://www-personal.umich.edu/~mejn/netdata
[8] M. Fiedler, "Algebraic connectivity of graphs," *Czechoslovak Mathematical Journal*, vol. 23, no. 98, pp. 298–305, 1973.
[9] L. Freeman, "A set of measures of centrality based on betweenness," *Sociometry*, vol. 40, pp. 35–41, 1977.
[10] G. Sabidussi, "The centrality index of a graph," *Psychometrika*, vol. 31, no. 4, pp. 581–603, 1966.
[11] M. Newman, *Networks: An Introduction*. Oxford University Press, Inc., 2010.
[12] M. Everett and S. P. Borgatti, "Ego network betweenness," *Social Networks*, vol. 27, no. 1, pp. 31–38, 2005.
[13] P.-Y. Chen and A. Hero, "Local Fiedler vector centrality for detection of deep and overlapping communities in networks," in *Proc. IEEE ICASSP*, 2014.

[14] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, "Attack vulnerability of complex networks," *Phys. Rev. E*, vol. 65, p. 056109, May 2002.
[15] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge University Press, 1990.