MOTIF-BASED ANALYSIS OF POWER GRID ROBUSTNESS UNDER ATTACKS

Asim Kumer Dey, Yulia R. Gel *

University of Texas at Dallas
Department of Mathematical Sciences
Richardson, TX 75080, USA

H. Vincent Poor

Princeton University
Department of Electrical Engineering
Princeton, NJ 08544, USA

ABSTRACT

Network motifs are often called the building blocks of networks. Analysis of motifs is found to be an indispensable tool for understanding *local* network structure, in contrast to measures based on node degree distribution and its functions that primarily address a *global* network topology. As a result, networks that are similar in terms of global topological properties may differ noticeably at a local level. In the context of power grids, this phenomenon of the impact of local structure has been recently documented in fragility analysis and power system classification. At the same time, most studies of power system networks still tend to focus on global topological measures of power grids, often failing to unveil hidden mechanisms behind vulnerability of real power systems and their dynamic response to malfunctions. In this paper a pilot study of motif-based analysis of power grid robustness under various types of intentional attacks is presented, with the goal of shedding light on local dynamics and vulnerability of power systems.

***Index Terms*—** Power grids, complex network, robustness, subgraphs, motifs, local topological properties

1. INTRODUCTION

The past decade has seen increasing interest in the application of tools developed in the interdisciplinary field of complex network (CN) analysis to improve our understanding of power system behavior (for overviews see, e.g., [1, 2, 3] and references therein). A power grid can be naturally described as a graph in which nodes represent, e.g., transformers, substations or generators, and edges represent electrical connections. There generally exist two main approaches to analysis of power systems using CN tools. The first approach is based on purely topological properties of a grid network, and the second hybrid approach aims to incorporate electrical engineering concepts, e.g. impedance, maximum power, etc, into the CN analysis, which typically results in a representation of a grid as a weighted directed graph. Both approaches provide important complementary insights into hidden mechanisms behind functionality of power systems, and neither approach can be viewed as a universally preferred method (see [2] for the detailed overview). In the current paper, we start our analysis from the viewpoint of topological grid properties.

Among the most widely explored topological characteristics of power grid networks are node degree distribution, mean degree, small world properties and, to a lesser extent, betweenness centrality measures – that is, primarily lower-order connectivity features that are investigated at the level of individual nodes and edges. However, a number of recent studies of power system reliability indices and stability estimation suggest that resilience of the power grid is also intrinsically connected to higher-order network features, or network *motifs* [4, 5]. The core idea is that if a particular subgraph structure such as, for instance, a triangle, star, square or wheel, occurs significantly often, then such a subgraph likely plays an important role in network functionality. And while higher-order network features have proven to play a fundamental role in understanding organization, functionality and hidden mechanisms behind many complex systems, from brain connectomes to protein-protein interactions to transportation congestion [6, 7, 8, 9], systematic analysis of network motifs in power grids and their impact on system resilience is still largely understudied [2, 4, 5, 10] but constitutes an emerging research direction.

In this paper we present a pilot study of motif-based analysis of power grid structural vulnerability under various types of intentional attacks. In particular, we consider the dynamics of 4-node connected motifs in six European power grids under three attack strategies, namely, attacked nodes are selected based on degree centrality, betweenness centralities or decreasing order of load (i.e., cascading failures). As a reference, we use a power grid fragility classification of [10] based on a tail function of the grid degree distribution, that is, the deviation of the observed grid cumulative degree distribution

*Yulia R. Gel has been partially supported by NSF DMS 1736368 and NSF IIS 1633331, and H. Vincent Poor has been partially supported by NSF DMS 1736417, NSF CMMI 1435778 and NSF ECCS-1549881. This material is also based in part upon work supported by DARPA. This work was initiated while the second two authors were Visiting Scholars at the Isaac Newton Institute for Mathematical Sciences, Cambridge, UK, under the support of EPSRC grant no EP/K032208/1. The authors would like to thank M. Rosas-Casals for providing the data for European power grids and Y. Chun for help with GIS data extraction.

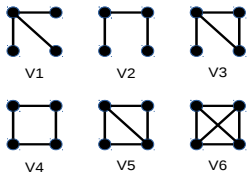

Fig. 1. All connected 4-node motifs.

from an exponential model. We find that local motif-based properties of fragile and robust networks noticeably differ in terms of their sensitivity to the type of attack. These pilot findings suggest that motifs can be useful metrics to characterize a level of power system vulnerability to various types of attacks and certain motifs can potentially serve as early warning indicators of system failure.

2. MOTIF-BASED ANALYSIS OF POWER GRIDS

Background on graphs We consider an undirected graph $G = (V, E)$ as a model of a power grid network. Here V is a set of nodes, and E is a set of edges. The order and size of G are defined as the number of nodes and edges in G, i.e., $|V|$ and $|E|$, respectively. We assume that if an edge $e_{uv} \in E$, then $u \neq v$. A graph G is connected if there exists a path from any node to any other node in G. The distance $d(u, v)$ is defined as the minimum path length from u to v in G. The degree of a node u is the number of edges incident to u.

A graph $G' = (V', E')$ is a *subgraph* of G (i.e., $G' \subseteq G$), if $V' \subseteq V$ and $E' \in E$. If $G' = (V', E')$ is a subgraph of G and E' contains all edges $e_{uv} \in E$ such that $u, v \in V'$, then G' is called an *induced* subgraph of G. Two graphs $G' = (V', E')$ and $G^{''} = (V^{''}, E^{''})$ are called *isomorphic* if there exists a bijection $h : V' \rightarrow V^{''}$ such that any two nodes u and v of G' are adjacent in G' if and only if $h(u)$ and $h(v)$ are adjacent in $G^{''}$.

Network motifs and their measures Analysis of higher-order structures of G, or multiple-node subgraphs, provides invaluable insights into network functionality and organization beyond the trivial scale of individual vertices and edges. A *motif* here is broadly defined as a recurrent multi-node subgraph pattern that tends to appear more often than would be expected in a randomized network. Network motifs were introduced by [6] in conjunction with the assessment of stability and robustness of biological networks, and later have been studied in a variety of contexts (for overviews see [9, 11]).

Formally, let $G_k = (V_k, G_k)$ be a k-node subgraph of G. If there exists an isomorphism between G_k and G', $G' \in G$, we say that there exists an *occurrence*, or *embedding* of G_k in G. A *motif signature* $f_G(G_k)$ is a number of occurrences of G_k in G. If a subgraph G_k occurs more frequently than expected by chance, it is called a network *motif* [6]. Figure 1 shows all connected 4-node motifs. The significance of motifs for a particular network can be measured by calculating motif concentrations and Z-scores. In Z-score the number of appearances of a motif in the observed network is compared with the corresponding quantity for a randomized network: $Z = M_R - M/s$, where M is the mean number of specific motif occurrences in B replicated randomized networks, s is the corresponding sample standard deviation, and M_R is the observed number of motifs in the specific power system network. In this study randomized networks are simulated using a configuration model [12]. The concentration (C_i) of n-node motif type i is the ratio between its number of appearances (N_i) and the total number of n-node motifs in the network: $C_i = N_i / \sum_i N_i$, where $\sum_i N_i$ is the total number of n-node motifs.

Conventional graph characteristics and vulnerability metrics The vulnerability of a power grid network can be described in terms of a drop in its performance when a disruptive event emerges. According to [2], the common topology-based vulnerability/robustness metrics are: degree distribution, average path length (APL), diameter (D), clustering coefficient (CC), betweenness centrality (BC), etc., as noted above.

The node degree of a network is characterized by a probability mass function $P(k)$ indicating the probability that a randomly selected node has k links. As suggested by [13], higher heterogeneity of power grids and, in particular, higher deviations from the Poisson distribution, tends to imply higher fragility. Power grid networks are assumed to follow exponential cumulative degree distributions [10]. That is, the probability that a node chosen uniformly at random has a degree k or higher follows: $P(K \geq k) = C \exp(-k/\gamma)$, where C is a normalization constant, k is the node degree and γ is a characteristic parameter. According to [13] and [10], a power grid is robust if $\gamma < 1.5$ and fragile if $\gamma > 1.5$.

Robustness under attacks In robustness under attacks, the aim is to evaluate how a network behaves when a fraction of random or selective nodes are removed. If the node to be removed at each step is selected at random, then the strategy is called a *random attack*. In the case of intentional attacks, the targeted nodes to be removed are selected based on their properties. For instance, if the nodes are selected in the decreasing order of their degree or betweenness centrality, the resulting attack is called a *degree based attack* or *betweenness based attack*, respectively. Finally, in a *cascading attack*, nodes are targeted in the decreasing order of their loads. Typically the vulnerability of a network is measured on the basis of the remaining connectivity, largest subgraph size, D, APL, etc., after each node removed with different attack strategies. In this study we focus on remaining motif distributions under different targeted attacks, e.g., degree based, betweenness based and cascade attacks. More specifically, our goal is to analyze the decay rate of a specific motif concentration under different types of attacks and enhance our understanding of local robustness properties of the corresponding network. Algorithm 1 provides an outline of how motif concentrations are calculated under degree based attacks. The method is similar

under betweenness based attacks, except V is sorted by descending order of betweenness centralities. Under cascading attacks, betweenness is recalculated after each node removal. Finally, under a random error (attack), nodes are removed randomly.

Algorithm 1: Degree based attack tolerance of networks based on motifs concentrations.

Input : Power grid $G = (V, E)$.
Output : Motif concentrations under targeted attacks.

N_k-number of V_k motif in G, $k = 1, \ldots, 5$;
Concentration, $C_k = N_k / \sum_k N_k$;
D_v-degree centrality of a node v. Calculate $D_v, \forall v \in V$;
$T(G) \leftarrow$ sorted V by D_v (descending) ;
for $i = 1$ **to** $|T(G)|$ **do**
    $V = V - T(i)$;
    $E = E - \{(x, y) \in E : x = T(i) \text{ or } y = T(i)\}$;
    Calculate N_k for $k = 1, \ldots, 5$;
    Calculate concentration $C_k[i] = N_k / \sum_k N_k$;
end;

3. CASE STUDIES

Data In this project we study electricity transmission networks of two European countries, e.g., Germany and Italy (the same power grid data analyzed by [14]), and four European power system operators, e.g., RTE, Amprion, 50 Hertz, and TenneT. The transmission network of Germany consists of 445 nodes (power stations/sub-stations) and 567 edges, and is the sparsest among the considered networks. The transmission network of Italy has 273 nodes and 375 edges. RTE is the French high-voltage transmission system, formed by 190 nodes and 224 edges. Amprion is one of the six transmission system operators in Germany, with 193 nodes and 252 edges. 50Hertz operates the transmission grid in the northern and eastern part of Germany, with a direct connection to Poland, the Czech Republic, and Denmark. The 50Hertz network has 63 nodes and 82 edges. Finally, TenneT operates in the Netherlands and Germany, and is formed by 79 nodes and 80 edges. Data for Germany and Italy are obtained from the Union for the Coordination of the Transmission of Electricity and data for the four system operators are obtained from the SciGRID [15].

Conventional CN robustness analysis Table 1 presents conventional network-based vulnerability metrics for the six power grids. Table 1 suggests that mean degree, APL, D, CC and BC for Germany, Italy, and TenneT tend to be lower than the respective metrics for RTE, Amprion and 50Hertz. In addition, Table 1 shows the estimated fragility parameter γ, resulting from approximating the cumulative degree distribution of each grid with an exponential model [13, 10]. We find that the electricity transmission system of Germany and Italy are robust with γ of 1.324 and 1.204, respectively. The TenneT power system is on the border of robustness with γ of 1.501. Finally, RTE, Amprion and 50Hertz tend to be fragile with $\gamma \approx 2$, and 50Hertz appears to be the most fragile grid with the highest γ of 2.13.

Table 1. Vulnerability metrics for the six power grids.

Power System	γ	Mean Degree	APL	D	CC	BC
Germany	1.32	2.58	11.75	30	0.07	2335.80
Italy	1.21	2.81	9.74	28	0.08	981.85
TenneT	1.50	2.03	5.33	12	0.10	78.71
RTE	1.86	2.36	8.05	20	0.17	379.91
Amprion	1.98	2.61	7.01	18	0.09	530.10
50Hertz	2.13	2.60	5.15	14	0.15	120.60

Motif-based robustness analysis We start from the concentrations and Z-scores for different 4-node motifs that appear in the six European power grids. Since motif distributions are highly skewed, standard z- and t-quantile are no longer appropriate. Hence, we compare the observed motif Z-scores with critical values obtained from parametric bootstrap under a configuration model as a reference. All grids but TenneT and 50Hertz, have statistically significant concentrations of V_1 to V_5 motifs, with respect to a reference configuration model. No grid exhibits a V_6 motif.

In cases of TenneT and 50Hertz, we find that both grids deliver non-significant concentrations of detour motifs (i.e., V_4 and V_5). At the same time, the more robust TenneT has also a non-significant concentrations of low connectivity tree-like *dead end* motifs, V_2; while the most fragile 50Hertz has a statistically significant concentration of a tree-like motif V_2.

Remarkably, in their studies of European power grid networks, the authors of [10] find that power system fragility seems to increase as the elements of the grid become more interconnected and the number of $\{3, 4\}$-node subgraph patterns such as stars and triplets, begins to increase. Independently, based on the analysis of synthetic power grids and a case study of the Northern European power system, [4] and [5] show that an abundance of tree-like dead-end 4-node subgraph patterns leads to a loss of stability and degradation of resilience. More recently, [16] which studies the impact of removing transmission lines with a high betweenness centrality, suggests that fewer connections imply higher security. Hence, the motif analysis of TenneT and 50Hertz may imply that there exists some balance in representation of low connectivity tree-like and detour motifs, resulting in a relatively stable system. However, there likely exists some functional nonlinear interaction among low connectivity and detour motifs and network robustness.

To assess the vulnerability of the six power grid networks, we investigate the dynamics of motif distributions under degree based targeted attacks. Fig. 2 shows the remaining motif concentrations after each node removed under degree based attacks. From Fig. 2, we find that motifs in the RTE and Amprion networks disappear more quickly as nodes are removed than do the motifs of the Germany and Italy networks. Fur-

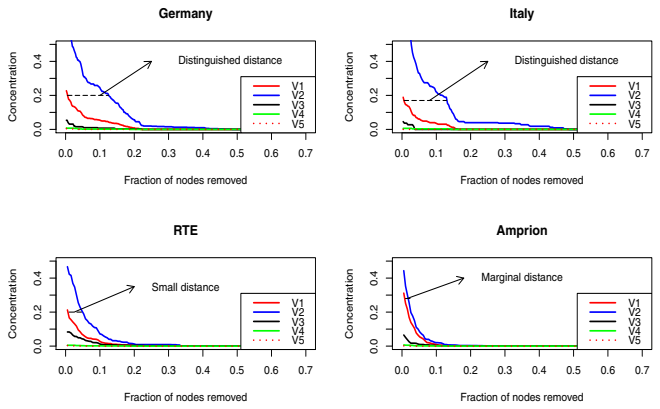

Fig. 2. Dynamics of 4-node motif concentrations under degree based attacks.

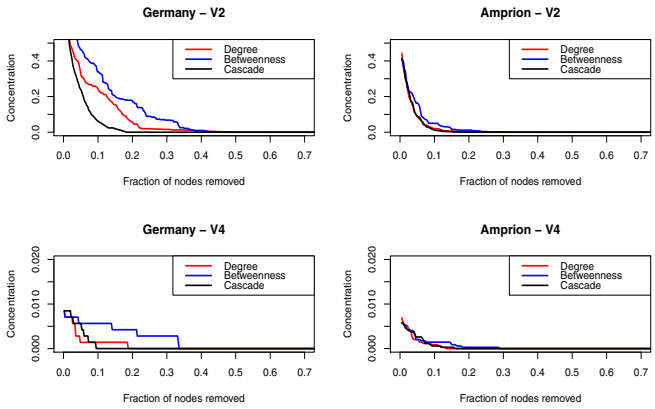

Fig. 3. Persistence of motif concentrations under different targeted attacks.

thermore, there is a marked distance among motif concentration curves in the Germany and Italy networks, whereas, the gap between curves in the RTE and Amprion networks are narrower. This also suggests that the motif disappearing rate for the Germany and Italy power grids are slower than those for the RTE and Amprion power grids. According to the results in Table 1, we know that the Germany and Italy power grids are robust but the RTE and Amprion power grids are fragile. Therefore we can say that the motifs disappear more quickly as the nodes are removed in the fragile networks than do motifs of the robust networks.

Furthermore, Fig. 3 shows that, for Germany, which is classified as a robust network, there exist significant differences among the decay rates of motif concentrations of V_2 and V_4 under different intentional attacks. However, for Amprion, which is classified as a fragile network, motif curves under all types of attacks are much closer to each other. These results suggest that the local motif structures of fragile and robust networks are sensitive with respect to the attack strategy and considered motif. Analysis for other types of networks (i.e., Italy, RTE, TenneT and 50Hertz), attacks and 4-node motifs are omitted for brevity, but mirror the conclusions above. (For the detailed study of all six power grids see [17]).

4. CONCLUSION AND DISCUSSION

Vulnerability of power systems is a very active research area, and grid robustness depends on many known and latent factors. Furthermore, notions of grid robustness are not universal, and the same grid can exhibit different vulnerability properties under different types of intentional attacks and random failures. In this paper we have investigated the dynamics of higher order topological properties of grid networks, namely, motifs, under various types of attacks. In particular, although even basic $\{3, 4\}$-node motifs have been proven to unravel hidden mechanisms behind functionality and stability of various complex systems (see [6, 11, 18] and reference therein), including a limited number of motif-based vulnerability studies in power networks [5, 10], to our knowledge, there exists no previous study of motif-based analysis of power systems under attacks. In this pilot study we have focused on motif-based analysis of local power grid vulnerability under random and intentional attacks. We have found that the dynamics of distributions of 4-node motifs under various attacks differ with respect to the global tail-based grid classification of power grid fragility proposed in [10]. In particular, we have found that robust and fragile power systems exhibit different degrees of local sensitivity and degradation with respect to the type of attack and the type of motif. Hence, motif characteristics such motif concentrations can be potentially used as alternative local metrics of fragility under attacks as well as early warning indicators of system degradation and failure. In the future, we plan to further expand this study into a hybrid analysis of local motif-based topological and functional properties of weighted power grid networks.

5. REFERENCES

[1] G. A. Pagani and M. Aiello, "The power grid as a complex network: A survey," *Physica A*, vol. 392, no. 11, pp. 2688–2700, 2013.

[2] L. Cuadra, S. Salcedo-Sanz, J. Del Ser, S. Jiménez-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.

[3] M. Rohden, D. Jung, S. Tamrakar, and S. Kettemann, "Cascading failures in AC electricity grids," *Physical Review E*, vol. 93, pp. 032209, 2007.

[4] P. J. Menck, J. Heitzig, J. Kurths, and H. J. Schellnhuber, "How dead ends undermine power grid stability," *Nature Communications*, vol. 5, pp. 3969, 2014.

[5] P. Schultz, J. Heitzig, and J. Kurths, "Detours around

basin stability in power networks," *New Journal of Physics*, vol. 16, no. 12, pp. 125001, 2014.

[6] R. Milo, S. Shen-Orr, S. Itzkovitz, N. Kashtan, D. Chklovskii, and U. Alon, "Network motifs: Simple building blocks of complex networks," *Science*, vol. 298, no. 5594, pp. 824–827, 2002.

[7] N. Pržulj, "Biological network comparison using graphlet degree distribution," *Bioinformatics*, vol. 23, no. 2, pp. e177–e183, 2007.

[8] A. R. Benson, D. F. Gleich, and J. Leskovec, "Tensor spectral clustering for partitioning higher-order network structures," in *Proc. SIAM SDM*, 2015, pp. 118–126.

[9] N. K. Ahmed, J. Neville, R. A. Rossi, N. Duffield, and T. L. Willke, "Graphlet decomposition: Framework, algorithms, and applications," *Knowledge and Information Systems (KAIS)*, vol. 50, pp. 1–32, 2016.

[10] M. Rosas-Casals and B. Corominas-Murtra, "Assessing European power grid reliability by means of topological measures," *WIT Transactions on Ecology and the Environment*, vol. 121, pp. 527–537, 2009.

[11] A. S. Schulz, M. Skutella, S. Stiller, and D. Wagner, *Gems of Combinatorial Optimization and Graph Algorithms*, Springer, 2015.

[12] E. D. Kolazcyk, *Statistical Analysis of Network Data*, Springer, 2009.

[13] R. V. Sóle, M. Rosas-Casals, B. Corominas-Murtra, and S. Valverde, "Robustness of the European power grids under intentional attack," *Physical Rev. E*, vol. 77, pp. 026102, 2008.

[14] L. Luo, E. Bompard, and Rosas M., "On the difficulty (and success) of correlating empirical data and (extended) topological measures in power grid networks," in *Proc. 7th Int. Conf. on Critical Inf. Infrastructure Security*, 2012, pp. 529–541.

[15] W. Medjroubi and C. Matke, *SciGRID – An Open Source Model of the European Power Transmission Network*, 2017.

[16] M. Mureddu, G. Caldarelli, A. Damiano, A. Scala, and H. Meyer-Ortmanns, "Islanding the power grid on the transmission level: Less connections for more security," *Scientific Reports*, vol. 6, pp. 34797, 2016.

[17] A. K. Dey, Y. R. Gel, and H. V. Poor, "Motif-based analysis of power grid robustness under attacks," *http://arxiv.org/abs/1708.06738*, 2017.

[18] C. E. Tsourakakis, J. Pachocki, and M. Mitzenmacher, "Scalable motif-aware graph clustering," *arXiv:1606.06235*, 2016.