Understanding a Power Grid's Cyber-Physical Interdependence Through Higher-order Motifs

Hao Huang *Member, IEEE*[*], H. Vincent Poor, *Fellow, IEEE*[*], David Flynn, *Member, IEEE*[†],
Mohammad Al-Muhaini, *Senior Member, IEEE*[‡]
[*]Department of Electrical and Computer Engineering, Princeton University, Princeton, New Jersey, USA
[†]James Watt School of Engineering, University of Glasgow, Glasgow G12 8QQ, United Kingdom
[‡]Electrical Engineering Department, King Fahd University of Petroleum & Minerals, Eastern Province, Saudi Arabia
Email: hh6219@princeton.edu, poor@princeton.edu, david.flynn@glasgow.ac.uk, muhaini@kfupm.edu.sa

***Abstract*—Power grid consists of interconnected cyber and physical networks. The complexity of which is increasing as a result several factors including: the convergence of low carbon technologies, the increased coupling of other critical networks, and a need for new distributed control and forecasting capabilities. These trends are creating unprecedented complexity in our critical networks, as well as introducing new threats to their functionalities. Hence, the network design is crucial to ensure the power grid's inherent security and resilience. Given its multilayered nature, this necessitates an understanding of the interdependence between cyber and physical networks. However, the heterogeneity between these networks makes it challenging to holistically analyze the power grid's cyber-physical architecture without losing granularity. To address this, higher-order motifs, defined as small connected subgraphs, can be employed to disclose the topological interdependence of heterogeneous networks at a local level. This paper uses an augmented cyber-physical WSCC 9-Bus System to investigate its 4-node motif patterns under different cyber attack scenarios. Certain 4-node motifs demonstrate their necessity to secure power grid functionality.**

***Index Terms*—Resilient Power Grid, Higher-order Motifs, Cyber-Physical Network, Cybersecurity, Resilience**

I. Introduction

The modern power grid is a multilayered, interdependent network where cyber and physical systems are interconnected. With the integration of renewable energy sources (RES) and bi-directional energy transaction toward a decarbonized grid, human and weather factors play an increasingly important role in maintaining the functionality of the power grid. The growing diversity in energy generation, especially through the highly distributed integration of intermittent RES, and more dynamic and decentralized energy networks necessitate that the cyber physical network of power grids must maintain critical network services, whilst analysing an increasingly stochastic and complex network of cyber and physical assets [1]. Cyber-physical networks can enable rapid decarbonisation, improved services, reduction in energy costs, improved resilience and enhanced accessibility to energy services. However, such complex and coupled cyber and physical networks can create risks to coupled networks and present new vulnerabilities e.g. cyber attacks, if not designed appropriately. Network topology lays the foundation for the power grid's resilience and security [2]. Given the power grid's multilayered nature, this calls for a holistic understanding and design of the power grid's cyber-physical network to improve its inherent resilience.

It is intrinsically challenging to capture the interdependence between cyber and physical networks due to the heterogeneity of their network structures and functionalities. However, both cyber and physical networks can be modeled with graphs where nodes and edges are assigned with different values to represent their attributes. The cyber-physical power grid can be viewed as two interconnected graphs that interact with each other. By leveraging the graph representation and topological properties, various graph-theoretic approaches have been used to evaluate the risk, reliability, and robustness of cyber-physical power systems against adversaries from the cyber and physical domains. For example, Umunnakwe *et al.* have used betweenness centrality, considering the cyber-physical graphs, to evaluate the risk and vulnerability of components in the power grid [3]. Huang *et al.* have applied ecological network analysis to cyber-physical power systems to evaluate their robustness and resilience with different cyber network structures [4]. Zhou *et al.* have used weighted spectral analysis on cyber-physical power systems to quantify resilience against cyber attacks [5]. The metrics and methodologies used in the aforementioned works primarily use lower-order connectivity features that aggregate the properties of individual nodes and edges in the system. The interdependence between cyber and physical networks cannot be clearly captured or understood.

Higher-order motifs are defined as patterns of interconnections or subgraphs occurring in complex networks at numbers that are significantly higher than those in randomized networks [6]. Recognizing higher-order motifs embedded in a larger network could indicate the presence of evolutionary design principles or have an overly influential role on system-wide dynamics [7]. Analysis of higher-order motifs can provide invaluable insights into network functionality and organization beyond trivial scale studies on individual nodes and edges. Several works have utilized higher-order motifs to study and evaluate the robustness, reliability, and resilience of power networks against cascading failures [8]–[10]. Motif patterns can also help operators efficiently identify the list of *N-k* contingencies in power systems [11]. Although these works only apply the motif-based analyses on the physical network, there is a significant potential to utilize higher-order motifs for understanding local network structure within multilayered networks, such as cyber-physical power systems, accounting for their interdependence.

The research question raised in this paper is *"what can higher-order motifs inform about the interdependence between cyber and physical networks in the modern power grid? "* This paper presents a preliminary study utilizing *all connected 4-node motifs* to characterize the topological interdependence between cyber and physical networks in the power grid under different cyber attacks based on their network properties. By comparing motif dynamics at different domains and power grid's functionality during cyber attacks, we can observe that certain 4-node motif pattern (M_2, M_3, and M_4) are crucial for the cyber-physical power grid's security and resilience.

The rest of the paper is organized as follows: Section II reviews the concepts and applications of higher-order motifs in network studies. Section III introduces a topological importance-based cyber attack algorithm, which launches cyber attacks to compromise the functionalities of cyber-physical power grids. Section IV demonstrates case studies of higher-order motif on the cyber-physical WSCC 9-bus power grid under cyber attacks. Section V presents the key findings and introduces future research.

II. Higher-Order Motifs

Higher-order motifs were initially used to analyze the structural properties of ecological food webs and neuron networks. They are recurrent and statistically significant subgraphs or patterns of a larger graph [6]. Let $G = (V, E)$ be an undirected graph, where V is the set of nodes and E is the set of edges. The order and size of G are defined as $|V|$ and $|E|$, which are the number of nodes and edges, respectively. A graph $G' = (V', E')$ is a subgraph of G, if $V' \subseteq V$ and $E' \subseteq E$. 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 an *induced* subgraph of G. Two graphs $G' = (V', E')$ and $G'' = (V'', E'')$ are called *isomorphic* if there exists a bijection h: $V' \to V''$ 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''. A motif $G' = (V', E')$ is defined as a recurrent multiple-node subgraph pattern, which is a n-node subgraph of G, where $|V'|$ is n. If there exists an isomorphism between G' and G'', $G'' \in G$, we say that there exists an occurrence or embedding of G' in G.

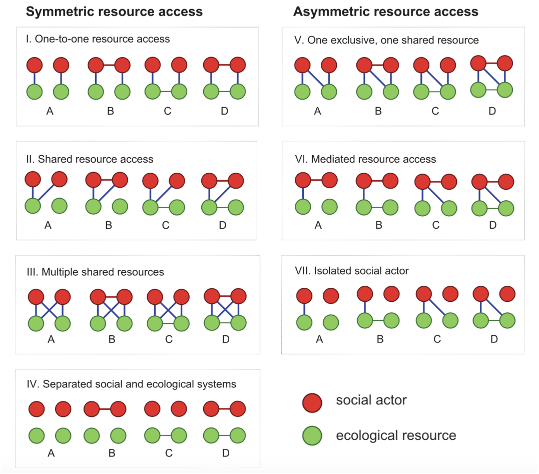

Symmetric resource access
Asymmetric resource access
I. One-to-one resource access
II. Shared resource access
III. Multiple shared resources
IV. Separated social and ecological systems
V. One exclusive, one shared resource
VI. Mediated resource access
VII. Isolated social actor
A
B
C
D
social actor
ecological resource

Fig. 1: Seven different Social-Ecological Systems motif families [12].

The 4-node motifs have been used to disentangle intangible social–ecological systems. In order to understand the social-ecological interdependencies, Bodin and Tengö utilized the 4-node motifs where two nodes are from social systems (social actors) and two nodes are from ecological systems (ecological resources) [12]. Fig. 1 shows all possible patterns of interdependence between social and ecological systems, considering the direction of connectivity between social and ecological systems. Both social-ecological systems and cyber-physical systems are multilayered networks. Intuitively, the patterns of interdependence between social and ecological systems could also be employed to understand the interdependence between cyber and physical networks at their boundaries. Fig. 1 also illustrates how the complexity of cyber-physical networks grows with the variability (type) and scale of assets. Given that, these networks, as per the introduction, need to tackle an increasingly more complex system of systems.

In this paper, we focus on all connected 4-node motifs shown in Fig. 2. The dynamics of these local structures have been shown to be related to the resilience and reliability of power grid and complex networks under intentional attacks [10]. The significance of motifs for a particular network can be assessed by motif concentration (C_i), which associates with the robustness and reliability of power networks. The C_i of a n-node motif of the type i motif is the ratio of its number of occurrences (N_i) to the total number of n-node motifs in the network. The formulation is $C_i = \frac{N_i}{\sum_i N_i}$, where $\sum_i N_i$ is the total occurrence of all n-node motifs in the original network.

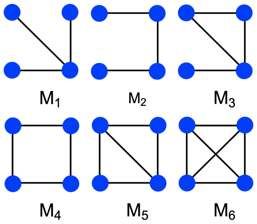


Fig. 2: All connected 4-node motifs.

In the following analyses, we examine the dynamics of 4-node motifs in cyber, physical, and cyber-physical networks under different cyber attacks considering their network properties of node degree, closeness centrality, and betweenness centrality, respectively. Besides, the social-ecological systems motifs are also employed to study the interdependence at the boundary between cyber and physical networks. This boundary is referred to as the *cyber-physical connection*, where two nodes are from cyber networks and two nodes are from physical networks.

III. Threat Model in Cyber Networks

This paper focuses on intentional cyber attacks. It assumes the adversary has infiltrated the cyber network and can exploit all available resources to achieve his/her goal [13]. The attack procedures are outlined in Algorithm 1. Based on the topological importance of cyber nodes, the adversary targets the most important cyber node and removes it along with all connected edges. Once the cyber attack reaches protective relays, which controls and monitors physical networks, the connected physical component is also removed from the physical network. This action can result in a physical disturbance affecting the operation of the power system. During each cyber attack, it will record the 4-node motifs in different networks and store the removed physical component for simulating disturbances.

For the importance calculation, this paper considers three network properties including node degree, closeness centrality, and betweenness centrality. Node degree (*ND*) is the number of edges adjacent to the node, which can be formulated as

Algorithm 1 Importance Based Cyber Attack

```
Input = Cyber Network Topology, $G_{cy}$ = ($V_{cy}$, $E_{cy}$)
Calculate Importance ($Imp_v$) of nodes in $V_{cy}$
$H(G_{cy})$ is the sorted $V_{cy}$ by descending $Imp_v$
for $t$ = 1 to $|H(G_{cy})|$ do
    $V_{cy}$ = $V_{cy}$ -$H(G_{cy})(t)$
    $E_{cy}$ = $E_{cy}$ - (x,y) $\in$ $E_{cy}$: x = $H(G_{cy})(t)$ or y = $H(G_{cy})(t)$
    if $H(G_{cy})(t)$ is $R_i$ (protective relay) then
        $E_{phy}$ = $E_{phy}$ - (a,b) $\in$ $E_{phy}$: a $\rightarrow$ $R_i$ or b $\rightarrow$ $R_i$
    end if
    Count 4-node motifs in different networks.
    Store the removed physical component for validation.
end for
```

$ND(v) = \sum_u a_{v,u}$, where $a_{u,v}$ is the entries of adjacency matrix. The higher value of *ND* means the node is more densely connected. Closeness centrality (*CC*) is a measure of centrality in a network, calculated as the reciprocal of the average length of the shortest paths between the node and all other nodes in the graph [14]. The more central a node is, the closer it is to all other nodes. *CC* of a node (v) can be expressed as $CC(v) = \frac{|V|-1}{\sum_u d(u,v)}$, where $d(u,v)$ is the length of the shortest path between vertices v and u. Betweenness centrality (*BC*) measures the extent to which a vertex lies on paths between other vertices [15]. Vertices with high betweenness may have considerable influence within a network since more paths that connect different vertices pass through them. *BC* of a node (v) can be expressed as $BC(v) = \sum_{s,t \in V, s \neq t \neq v} \frac{\sigma_{s,t}(v)}{\sigma_{s,t}}$, where $\sigma_{s,t}(v)$ is the number of shortest paths in the graph between s and t that contain node v, and $\sigma_{s,t}$ represents the number of shortest paths in the graph between s and t.

IV. Case Study on A Cyber-Physical WSCC-9 Bus System

A. Network Topology

Previously, cyber-physical power system studies often assume that cyber and physical networks have the same or similar topological structure, which overlooks many important details in both networks. The detailed cyber architecture of intelligent electronic devices and communication devices is essential to protect power grid [17]. It should be integrated with the physical network for a comprehensive analysis and design against unforeseen events. To provide a holistic view of cyber-physical topology, Hossain *et al.* built an augmented communication network with various types of cyber nodes for WSCC 9-bus system [16]. The augmented cyber network has detailed representations of cyber components including protective relays (**R**), routers (**r**), switches (**SW**), firewall (**FW**) and computer nodes of human machine interface (**HMI**) and control centers (**CC**) for the physical network. This cyber network also considers the redundancy of communication devices. Fig. 3 shows the physical network, cyber network, and cyber-physical network of WSCC 9-bus system.

B. Motif Concentrations Under Cyber Attacks

To investigate the interdependence between cyber and physical networks, the cyber-physical WSCC 9-bus system is modeled as *undirected* graph $G_{cps} = (V_{cps}, E_{cps})$, where V_{cps} is a set of nodes and E_{cps} is a set of edges in both cyber and physical networks. By applying attack scenarios in Algoritm 1, we can observe motif dynamics in different networks.

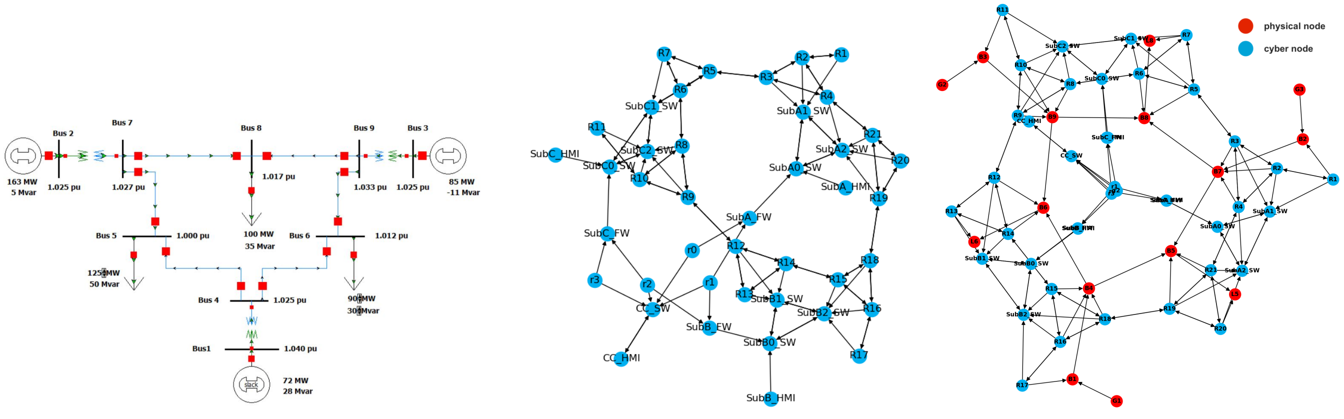
Fig. 4-7 show the dynamics of motif concentrations in cyber network, physical network, cyber-physical network, and cyber-physical connections under different attack scenarios, respectively. For the cyber-physical connection, we only consider the *all-connected* 4-node motifs from the seven social-ecological systems motif family in [12]. There are four motifs existing in the cyber-physical WSCC 9-bus system, which are *I.C*, *I.D*, *II.D*, and *VI.B*. Both *I.C* and *VI.B* are M$_2$ in Fig 2 but with different connectivities between cyber and physical networks, *II.D* is M$_3$, and *I.D* is M$_4$. With the saved information, the physical disturbance (disconnect branches, loads, and generators) can be simulated to examine the system's functionality without remedial actions. The *"Physical Network Breakdown"*, specified by the black dash lines in figures, shows the period from the initial physical disturbance triggered by cyber attacks until all loads are not supplied by the system or the system is blackout (whichever comes first).

It can be observed that M$_2$ and M$_3$ dominate cyber-physical network, cyber network, and cyber-physical connections with the highest motif concentrations, while M$_2$ and M$_1$ dominate the physical network. These differences stem from the connectivity and size of the networks. It is obvious that cyber network is more densely connected than physical network. Given that the size and order of the cyber network are larger than those of the physical network, the network properties of the cyber-physical network are closer to the cyber network.

Under different attack scenarios, the initial physical disturbances and the duration of *physical network breakdown* vary significantly. The *ND*-based attack gradually disconnects the cyber network until only a few 4-node motifs remain (all motif concentrations are below 0.1). This results in weak connectivity between the cyber and physical networks through protective relays. Any further attack can trigger cascading failures in physical network. This is evident in the sharp decay rate of C$_2$ in physical network, as shown in Fig. 6(a). The *CC*-based attack induces the physical disturbances earlier than *ND*-based attack. Some 4-node motifs in the cyber network still remain, and C$_2$ and C$_3$ are higher than 0.1 but lower than 0.3. Despite the early onset of physical disturbances, Fig. 6(b) shows that there are some stages where C$_2$ and C$_1$ remain unaffected, indicating that power systems' functionality is not deteriorated. The *BC*-based attack initiates the physical disturbance earliest, and the duration of *physical network breakdown* is also the longest. When the physical disturbance happened, most 4-node motifs still exist in the cyber network. There are also more unaffected stages in Fig. 6(c).

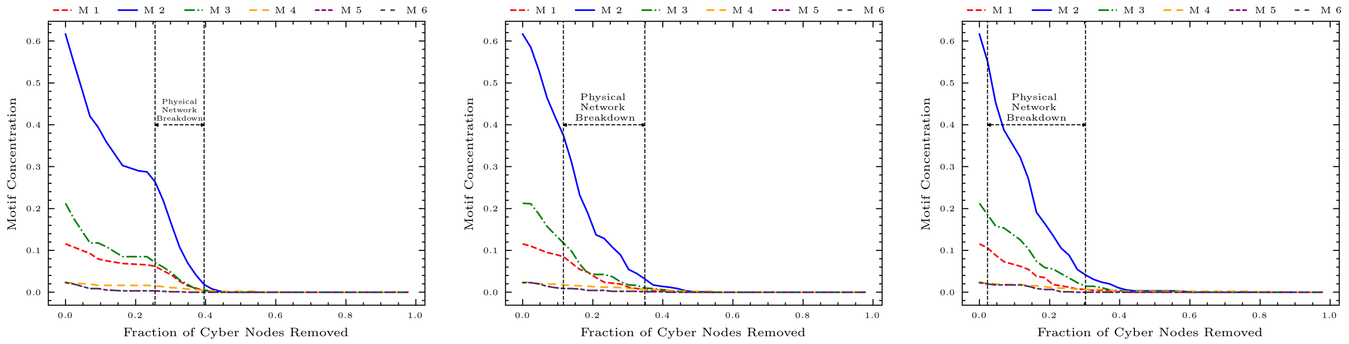
The motifs at the boundary between the cyber and physical networks exhibit intriguing patterns. Under all attack scenarios, the *physical network breakdown* is triggered by the decrease of M$_2$, M$_3$ and M$_4$. The M$_2$ is *I.C* in Fig. 1, wherein two cyber nodes are connected and each one controls a physical device. Since protective relays bridge the cyber and physical network, the reduction of above motifs can indicate the potential risk of cascading failures and disturbances on power systems' functionalities.

Based on the results, we observe that the 4-node motifs,



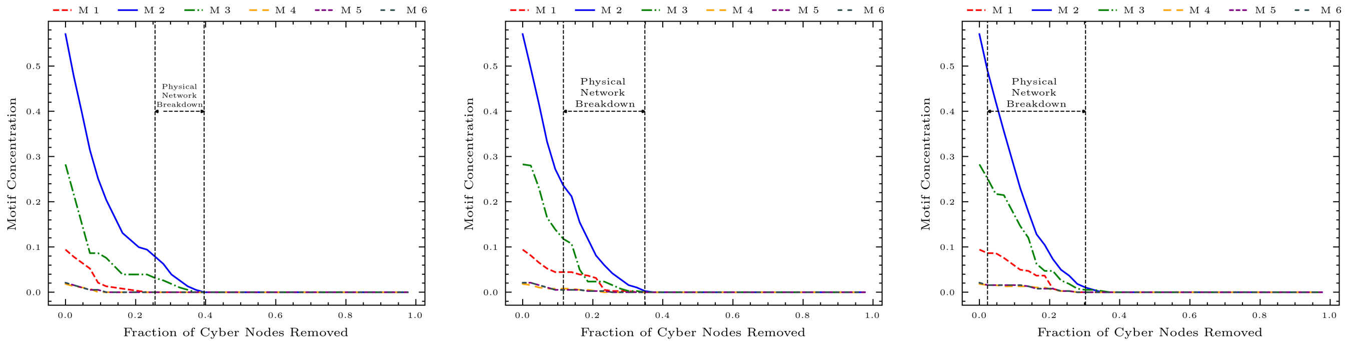
(a) Physical Network (b) Cyber Network (c) Cyber-Physical Network

Fig. 3: WSCC-9 Bus Cyber-Physical Power Grid [16]



(a) Node Degree-based Attack (b) Closeness Centrality-based Attack (c) Betweenness Centrality-based Attack

Fig. 4: Motif Concentration on the WSCC 9-Bus Cyber-Physical Network Under Different Cyber Attacks



(a) Node Degree-based Attack (b) Closeness Centrality-based Attack (c) Betweenness Centrality-based Attack

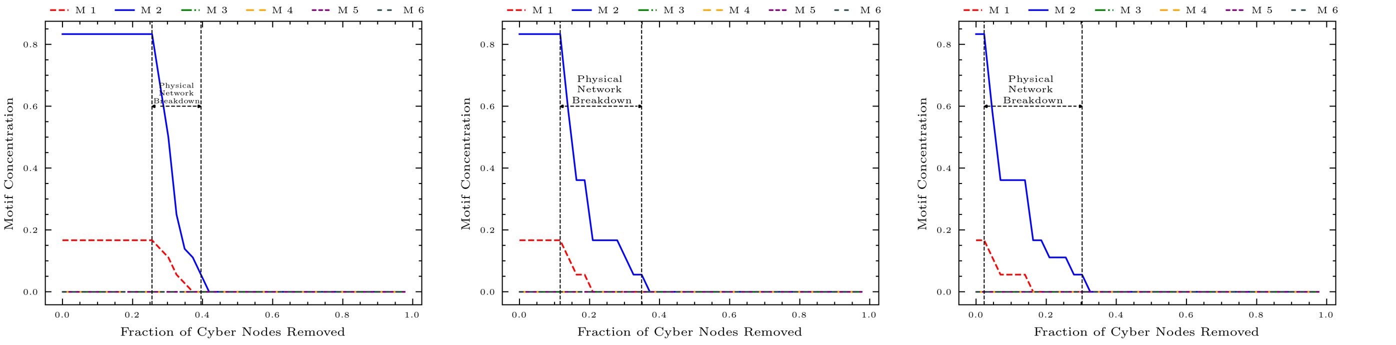
Fig. 5: Motif Concentration on the WSCC 9-Bus Cyber Network Under Different Cyber Attacks

particularly M_2, M_3 and M_4, can represent the resilience and reliability of the cyber-physical power grid against cyber attacks. A higher percentage of M_2 and M_3 in the system indicates that the cyber-physical network possesses greater resistance to prevent cyber attack from disrupting physical network and thus maintain the functionality of power systems. It also demonstrates that cyber resilience is paramount for the power grid's functionality. Inspecting M_2, M_3 and M_4 at the boundary of the cyber and physical networks can provide valuable information about potential risks within the system.

V. Conclusion and Future Work

This paper has presented a preliminary study of using higher-order motifs to understand the interdependence between cyber and physical networks in the power grid. With a detailed cyber-physical power grid, we utilized three cyber attack strategies to investigate the dynamics of motif concentrations in the cyber-physical power grid. The results show that M_2, M_3, and M_4 are key factors that ensure the security and functionality of the power grid against malicious activities in cyber networks. Especially for the cyber-physical connections, the reduction of the aforementioned motifs coincides with inducing physical disturbances.

In future work, we plan to investigate larger and more realistic cyber-physical power systems to further examine their higher-order motifs under events from different domains. The growth of RES and electric vehicles in the power grid can incur unpredictable fluctuations on power flows and a large amount

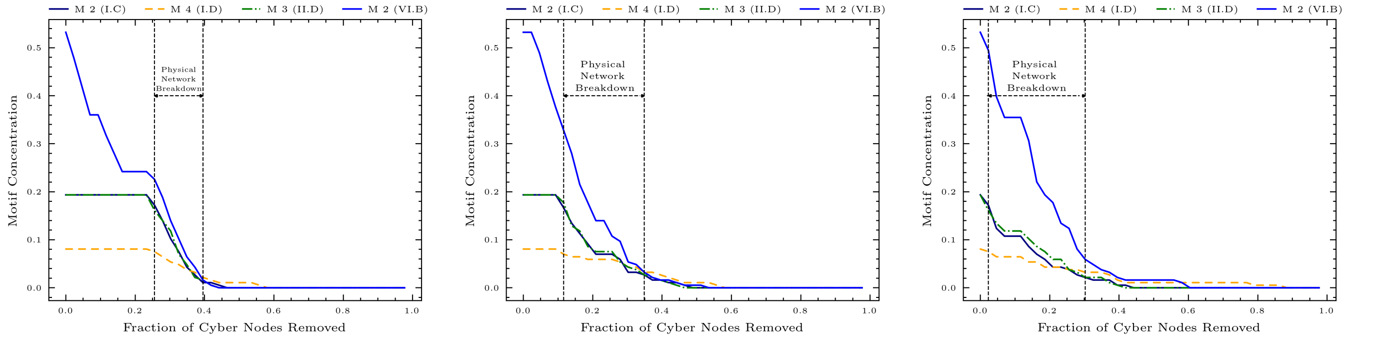


(a) Node Degree-based Attack

(b) Closeness Centrality-based Attack

(c) Betweenness Centrality-based Attack

Fig. 6: Motif Concentration on the WSCC 9-Bus Physical Network Under Different Cyber Attacks



(a) Node Degree-based Attack

(b) Closeness Centrality-based Attack

(c) Betweenness Centrality-based Attack

Fig. 7: Motif Concentration on the WSCC 9-Bus Cyber-Physical Connections Under Different Cyber Attacks

of data being transferred over the network. Such situations can introduce new threat vectors. With more investigations, there is a great potential to generalize the application of higher-order motifs to comprehend and guide the design of multilayered cyber-physical power grid with other interconnected critical infrastructures, such as transportation networks and gas networks, for their security and resilience.

ACKNOWLEDGMENT

The authors would like to acknowledge the National Science Foundation under Grant 2039716, a grant from the C3.ai Digital Transformation Institute, and the EPSRC grant EP/X038823/1 for their support.

REFERENCES

[1] L. L. Pullum, A. Jindal, M. Roopaei, A. Diggewadi, M. Andoni, A. Zobaa, A. Alam, A. Bani-Ahmed, Y. Ngo, S. Vyas *et al.*, *Big data analytics in the smart grid: Big data analytics, machine learning and artificial intelligence in the smart grid: Introduction, benefits, challenges and issues*. IEEE, Feb 2018.

[2] M. Panteli, D. N. Trakas, P. Mancarella, and N. D. Hatziargyriou, "Power systems resilience assessment: Hardening and smart operational enhancement strategies," *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1202–1213, 2017.

[3] A. Umunnakwe, A. Sahu, M. R. Narimani, K. Davis, and S. Zonouz, "Cyber-physical component ranking for risk sensitivity analysis using betweenness centrality," *IET Cyber-Physical Systems: Theory & Applications*, vol. 6, no. 3, pp. 139–150, 2021.

[4] H. Huang, A. Chatterjee, A. Layton, and K. Davis, "An investigation into ecological network analysis for cyber-physical power systems," in *Proceedings of 2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2021, pp. 252–257.

[5] H. Zhou, Z. Shen, and Z. Li, "Evaluating the resilience of cyber–physical power systems by weighted spectral analysis," *Energy Reports*, vol. 8, pp. 111–120, 2022.

[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] L. Stone, D. Simberloff, and Y. Artzy-Randrup, "Network motifs and their origins," *PLoS Computational Biology*, vol. 15, no. 4, p. e1006749, 2019.

[8] Q. Chen, H. Ren, C. Sun, Z. Mi, and D. Watts, "Network motif as an indicator for cascading outages due to the decrease of connectivity," in *The Proceedings of 2017 IEEE Power & Energy Society General Meeting*. IEEE, 2017, pp. 1–5.

[9] A. K. Dey, Y. R. Gel, and H. V. Poor, "Motif-based analysis of power grid robustness under attacks," in *Proceedings of 2017 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*. IEEE, 2017, pp. 1015–1019.

[10] ——, "What network motifs tell us about resilience and reliability of complex networks," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 116, no. 39, pp. 19 368–19 373, 2019.

[11] K. Zhou, I. Dobson, and Z. Wang, "The most frequent nk line outages occur in motifs that can improve contingency selection," *IEEE Transactions on Power Systems*, 2023 (Early Access).

[12] Ö. Bodin and M. Tengö, "Disentangling intangible social–ecological systems," *Global Environmental Change*, vol. 22, no. 2, pp. 430–439, 2012.

[13] M. J. Assante and R. M. Lee, "The industrial control system cyber kill chain," *SANS Institute InfoSec Reading Room*, vol. 1, p. 24, 2015.

[14] L. C. Freeman, "Centrality in social networks conceptual clarification," *Social Networks*, vol. 1, pp. 215–239, 1978. [Online]. Available: https://api.semanticscholar.org/CorpusID:751590

[15] U. Brandes, "On variants of shortest-path betweenness centrality and their generic computation," *Social Networks*, vol. 30, no. 2, pp. 136–145, 2008.

[16] S. Hossain-McKenzie, N. Jacobs, A. Summers, R. Adams, C. Goes, A. Chatterjee, A. Layton, K. Davis, and H. Huang, "Towards the characterization of cyber-physical system interdependencies in the electric grid," in *Proceedings of 2023 IEEE Power and Energy Conference at Illinois (PECI)*. IEEE, 2023, pp. 1–8.

[17] H. Huang, P. Wlazlo, Z. Mao, A. Sahu, K. Davis, A. Goulart, S. Zonouz, and C. M. Davis, "Cyberattack defense with cyber-physical alert and control logic in industrial controllers," *IEEE Transactions on Industry Applications*, vol. 58, no. 5, pp. 5921–5934, 2022.