Insight Into Cyber Information Flow Interdependencies Using Bio-inspired Topologies

Emily Payne, *Student Member, IEEE,* Shining Sun, *Student Member, IEEE,* Astrid Layton, *Member, IEEE*
Katherine Davis, *Senior Member, IEEE,* Shamina Hossain-McKenzie, *Member, IEEE*
Nicholas Jacobs, *Member, IEEE*

2024 58th Annual Conference on Information Sciences and Systems (CISS) | 979-8-3503-6929-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/CISS59072.2024.10480172

***Abstract*—With a power systems cyber network being targeted more than ever it is imperative to evaluate current and future power system designs. Bio-inspired designs previously applied to power systems have succeeded in creating a more resilient physical network. Here a cyber-information flow n etwork is modeled for the WSCC 9-bus system to analyze system resilience. Ecological Network Analysis is applied to improve the modeling of inter-cyber information flow t opologies a nd a ssess t heir resilience, risks, and vulnerabilities. Two disturbance scenarios are created to provide insight into network resilience and topological strength specifically r egarding n etwork c ommunication. The results suggest that Relay-to-Control Center information flows are more vulnerable to a disturbance. This supports a need for device redundancy in the overall information flow t opology. The results lay the foundation for future investigations into inter-cyber network interdependencies and the optimization of power grid system designs.**

***Index Terms*—Bio-inspired system design, network topology, cyber-physical interdependencies, cyber attacks, resilience, power grids**

I. Introduction

Modern technologies are revolutionizing power systems, improving their control and making them more interconnected but also leaving them increasingly susceptible to cyber attacks. The rapid adoption of emerging technologies is creating a fertile ground for cyber threats, such as Denial-of-Service (DoS), Man-in-the-Middle (MiTM) [1], and malware attacks [2]. A prime example of this growing vulnerability is the recent report from the Ukrainian Computer Emergency Response Team (CERT) [3]. They detail the repeated targeting of their energy infrastructure monitoring systems, showcasing the unexpected potential of cyber disruptions to influence physical components and ultimately lead to costly blackouts. Addressing these significant c hallenges n ecessitates a holistic approach to cyber-physical systems by first f ocusing o n the intricate interdependencies at play during security breaches and disturbances.

E. Payne, S. Sun, A. Layton, K. Davis are with Texas A&M University, College Station, Texas, USA. S. Hossain-McKenzie, N. Jacobs are with Sandia National Laboratory. Sandia National Laboratory is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

Traditional methods of handling power system emergencies rely on grid operators and hazard operation plans. Operators are trained to deal with emergencies to prevent blackouts [4] yet their operation departments often have minimal cooperation and collaboration with cyber departments [5]. A structural gap exists between power systems' Operational Technology (OT) and Information Technology (IT). Current strategies for handling emergencies in cyber-physical systems (CPS) are evolving but still in their infancy, highlighting the need for integrated and well-conceived plans that bridge this OT-IT divide [6]. Such plans are essential for developing more resilient and reliable power systems and preventing previous major US incidents.

Biological ecosystems on the other hand have demonstrated remarkable resilience in the face of disturbances, a quality captured by ecologists studying network architecture [7] and applied to human networks by engineering researchers. Ecological Network Analysis (ENA), which features quantitative metrics relating network characteristics to their functioning, has been applied to human networks such as supply chains [8], systems of systems [9], water distribution networks [10], and industrial resource networks [11]. These works however have primarily concentrated on physical networks, including power systems [12]–[15], aiming to emulate ecosystem resilience. These studies have used several ENA metrics, including Ecological Robustness (R_{ECO}), Average Mutual Information (*AMI*), Cyclicity (λ_{max}), and Degree of System Order (*DoSO*), to evaluate and design physical power systems network structures. Following the successful characterization of cyber-physical power systems utilizing DeepWalk and bipartite network modeling methods [16], the cyber component connections of power systems are investigated to understand the strengths and vulnerabilities of the cyber network layer separately. Cyber network topologies are here modeled in a similar fashion to ecological food webs and evaluated using ENA [17] to assess the resilience, risks, and vulnerabilities related to the overall topology of cyber-physical systems.

Prior work has elaborated on the development of preliminary topologies for a cyber network [18], examining 2 distinct scenarios (in a 3-substation and an 8-substation cyber-physical system) and emphasizing the potential of an ENA-based approach. That work also stated a need to further enhance cyber topology modeling by adding more content to the overall system, including firewalls, substations, and relays, to enable advanced disturbance patterns to be observed and

provide insight into the inner workings of network resilience, robustness, and security. This work advances these previous studies by computing disturbances *specifically* applicable to communication connections, described in [16]. Packet delivery information and changes in topological structure are analyzed, providing new insight into the possible openings available to adversaries and their impact on the overall network's ability to function under duress. The main contributions of this paper are as follows:

1) A bio-inspired model for assessing the strengths and weaknesses of communication system interactions.
2) Evaluation of the WSCC 9-bus power system case study using ENA and related network methods.
3) Highlighting of the most resilient network structures and the most robust and reliable network designs and data routing approaches using ENA.

The following sections are organized as follows: Section II is the background and problem formulation, Section III is the methodology, Section IV is the results and discussion, and Section V is the conclusion and future work.

II. Background and Problem Formulation

A Denial of Service (DoS) attack is a particularly critical threat that targets communication networks by flooding the network with an overwhelming volume of traffic using protocols. A DoS attack overloads the processing of messages and effectively disrupts the flow of necessary operational data. This disruption can lead to a cascade of negative outcomes, from operational delays to a complete shutdown of system monitoring and control functions. The consequences of such an attack can be far-reaching, potentially resulting in power outages, compromised system security, and even safety hazards.

This study uses an augmented Western System Coordinating Council (WSCC) 9-bus System [19] as the primary case study. There are 3 substations in total, composed of generators (G), buses (B), and loads (L). The focus here however extends to the cyber layer of the WSCC 9-bus system. A reconstructed cyber topology is created, inspired by a previous topology [16] where all the backup routers are removed. Devices in this topology have the following functions: routers *(r)* act as intermediaries between networks, Human Machine Interfaces *(HMI)* provide system operators with real-time monitoring and control, Firewalls *(FW)* guard against unauthorized access and cyber intrusion, and Relays *(R)* serve cyber-physical components for system protection and data acquisition. The cyber network is created as a hierarchical system, as is shown in Fig. 1, which mirrors the real-world power system networks. Each substation is composed of Relays *(R)*, Firewalls *(FW)*, routers *(r)*, Ethernet Switches *(SW)*, and *HMI*. As is shown in Fig. 1, each is colored differently with its own control room, which aims to run local operations coherently with the control center and monitor the stability of the power system. A main control center oversees the control rooms, acting as the brain of the system, which is responsible for data analysis, synchronization of different substations, and coordination of power generation.

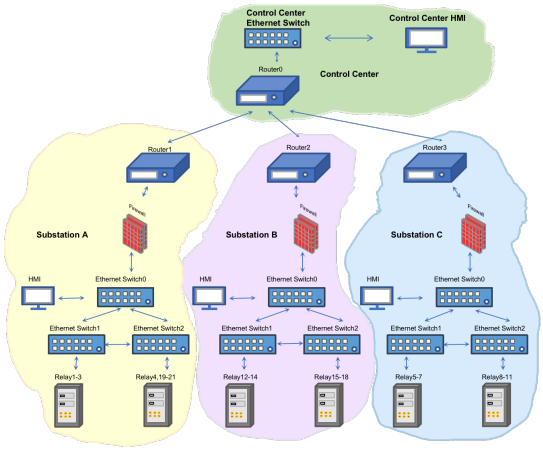

Fig. 1: WSCC-9 Bus System Cyber Topology, adapted from [16].

Several assumptions are made to analyze the information flows and the robustness of the cyber system. Firstly, the system here is analyzed based on a steady-state model. Secondly, cyber communication packets are modeled as discrete numerical values. For example, in Disturbance 1, the relay packet information begins as 1-per-relay in the system and is additive as it passes through other components/nodes. The cyber packets refer to digital data packets that carry crtitical information such as voltage magnitude, state of the breaker and the other electrical commands sent back from the operators.

The disturbance scenarios below highlight the diverse range of adversary targets. Within these scenarios, several different elements have been placed at risk in order to explore the system's response to singular or multiple actor (cyber element) type disturbances. All disturbance scenarios are modeled as a Denial of Service (DoS) attack to the following components:

- Disturbance 1: Relay 13 and Relay 20
- Disturbance 2: Communication between Relay 3 to Substation A's Ethernet Switch 1, Substation A's Ethernet Switch 0, and router 0

A. Sending Data

The objective of the cyber network's communication is to send data from the relays to the control center. Since both local and remote controls are controlled by the relays in this system, the data of the entire physical network is transmitted to both the respective local Human-Machine Interface (*HMI*) and the control center *HMI*. As we can see from the diagram in Fig. 2, the packets are calculated based on information flow.

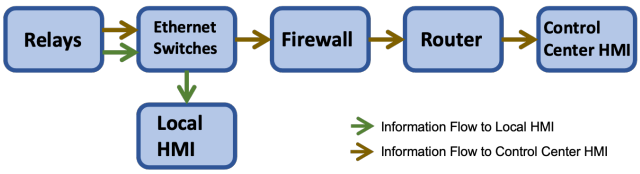

Fig. 2: Information Flow Diagram for One Way Sending Data

B. Delivering Commands

Fig. 3 demonstrates the information flow when delivering commands. The primary goal of the information flow is to facilitate the efficient transmission of commands, dispatched through localized and control center HMIs. Local and remote controls both issue the same types of commands, supporting the consistent and coherent operation of the network. However, a key distinction lies in the prioritization of these commands. While local commands, issued from the local HMI, are crucial for on-site management and immediate responses, commands from the control center, which oversees wider network operations and strategic decisions, take precedence during conflicts. This ensures that local operators can make real-time adjustments and respond to immediate needs in the field, while overall network strategy and security are the responsibility of the central control system.

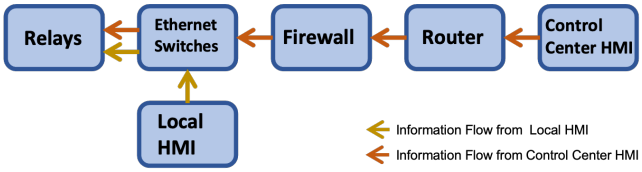

Fig. 3: Information Flow Diagram of One Way Delivering Command

III. Methodology

The analysis here includes Ecological Network Analysis (ENA) metrics, and traditional topology metrics including Average Node Degree (*ND*), Average Clustering Coefficient (*CC*), and Average Betweenness Centrality (*BC*) as calculated in [20], [21].

A. Ecological Network Analysis (ENA)

Prior work used ENA, which uses graph visualizations and matrix-based depictions to calculate quantitative network characteristics, to investigate a cyber-physical power network [22]. ENA uses two matrices, a structural food web [**F**] an *N*x*N* matrix where *N* is the number of actors or nodes inside the system boundaries, and an (*N*+3) x (*N*+3) flow magnitude-based matrix [**T**]. Figures 4 and 5 show a directional graph depiction of a cyber network for a power system and the flow matrix [**T**] for that same network, respectively, the latter of which includes system inputs, outputs, and dissipation beyond the selected system boundary [17], [23]–[25].

1) Flow Metrics: Ecological Fitness (R_{eco}, Eq. 1) is rooted in information and graph theory as well as statistics, based on the quantification of surprise and uncertainty. R_{eco} and it's related metrics identify unused energies within a network with respect to the highest possible effective performance [17]. Degree of System Order (*DoSO*, Eq. 2) is the independent metric within R_{eco} and is used by ecologists to quantify the organization, structure, and complexity of ecological food webs. The level of order and complexity within ecological food webs can have important implications for their stability, resilience, and ability to respond to disturbances [17].

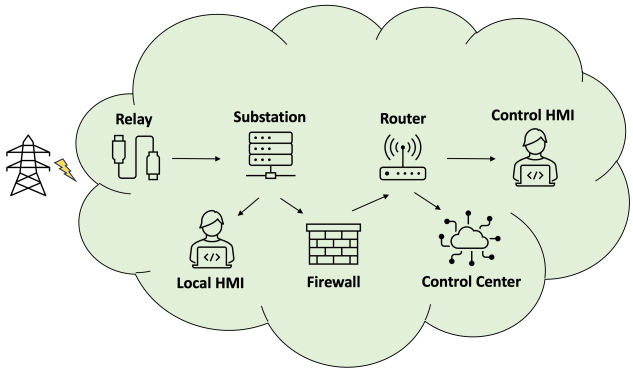

Fig. 4: A high-level directional graph for a cyber network of a power system. The cloud represents the system boundary.

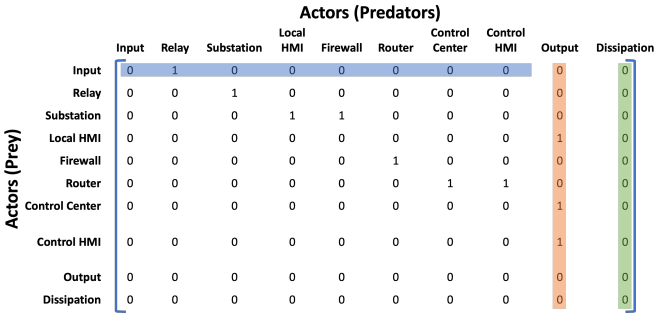

Fig. 5: The flow matrix [**T**] for the cyber network depicted in Fig. 4.

$$R_{\text{eco}} = -\left(DoSO\right)\log_e\left(DoSO\right) \tag{1}$$

$$DoSO = \left(\frac{AMI}{H}\right) \tag{2}$$

Ecologists, when plotting R_{eco} vs. *DoSO* for long-surviving food webs discovered what they now call the ecological Window of Vitality (*WoV*, Fig. 6) [7], [26]. Networks that form at the extreme values of *DoSO* (close to zero and one) are hypothesized as being those not fit to survive in nature, while peak fitness is observed within the ecological *WoV*, a range of approximately *DoSO* = 0.21-0.59 (the boundary is fuzzy).

Average Mutual Information (*AMI*) and the Shannon Index (*H*) are used to calculate *DoSO*. *AMI*, (Eq. 3) gauges the cumulative uncertainty concerning a flow's origin and subsequent direction, while *H* (Eq. 4) represents the maximum potential for organizational development within a flow network [16], [18]. Total System Throughput (*TSTp*) denotes system size, measured by the total energy units passing through the system (from inputs to outputs or the sum of the entire matrix [**T**]).

$$AMI = \sum_{i=1}^{N+3} \sum_{j=1}^{N+3} \frac{T_{ij}}{TSTp} \log_2 \left(\frac{T_{ij} \cdot TSTp}{T_i \cdot T_j} \right) \quad (3)$$

$$H = -\sum_{i=1}^{N+3} \sum_{j=1}^{N+3} \frac{T_{ij}}{TSTp} \log_2 \left(\frac{T_{ij}}{TSTp} \right) \quad (4)$$

$$E = H'/H_{max} \quad (5)$$

Evenness, also known as Species Evenness (E, Eq. 5), is a vital aspect of biodiversity and is mathematically assessed through various indices and metrics, with the well-known Shannon Evenness Index, also referred to as Pielou's Evenness Index [27], [28]. H_{max} in Eq. 5 denotes the maximum achievable value of the Shannon Index when all species have an equal abundance. An E value near 1 signifies a community exhibiting evenly distributed species without dominance. Inversely, a value substantially below 1 implies that certain species dominate, leading to an uneven network. Greater E has been found to correlate with increased stability and resilience in ecosystems, due to no single species exerting excessive influence and improved adaptability to alterations or disruptions. Low E on the other hand may render ecosystems susceptible to disturbances since any impact on a dominant species can significantly affect the entire community [28]–[31].

IV. Result and Discussion

The results provide some new insight regarding a cyber network's resilience and robustness against possible adversarial attack patterns. In this section, the results and discussion are presented together.

A. Ecological System Metrics

The results indicate that the *Relay-to-Control Center* topology is possibly less resilient than the *Control Center-to-Relay* topology. Figure 6 shows that all the *Relay-to-Control Center* topologies lie outside of the ecological *WoV*. This suggests that these system designs lack ecological similarity related to their resilience, instead having a higher level of pathway efficiency in their network design (*DoSO* closer to 1). This may correspond to the reporting mechanism enacted from the *Relay-to-Control Center* and suggests that creating more redundancy in the system, possibly via backup routers or relay-to-relay communications, would improve the network's response to disturbances. Notably, within this topology, all the disturbance scenarios have a lower *DoSO* than the undisturbed scenario, bringing them closer to the ecological *WoV*. This indicates that the disturbance is actually removing specific elements that cause lower redundancy, thereby creating a topology that is no longer a linear path. Disturbance 2 falls just shy of the ecological *WoV*, indicating that the cyber component loss of Relay 3 to Substation A's SW1 and Substation A's SW0, and router 0 may actually strengthen topology. This is due to all devices being weighted equally important. However, in actuality, it can be seen that the loss of a substation is a major concern as a device, but not in terms of creating system resilience.

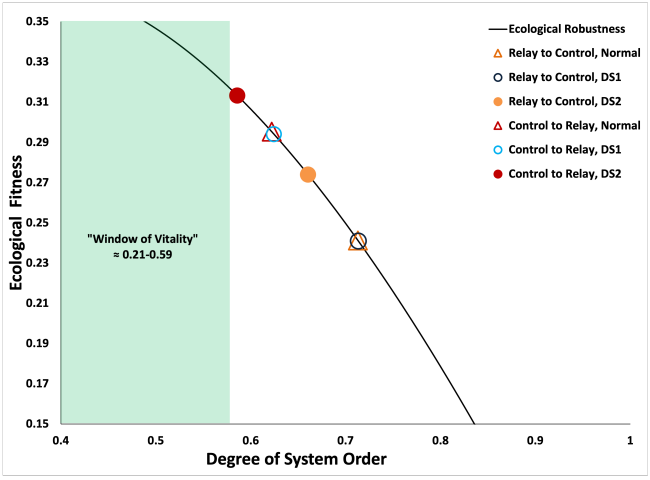

Fig. 6: Normal and disturbed cases plotted on the ecological fitness curve, with the ecological Window of Vitality highlighted in green. "Normal" indicates the fully operational/undisturbed case study, "DS" indicates disturbance scenario 1 or 2.

Similarly, the *Control Center-to-Relay* topology has the highest *DoSO* of the network in its non-disturbed state. Disturbance 2 moves the case study closest to the ecological *WoV*. Cyber components in both case studies with flows passing through them or concluding at them are at risk of an adversary targeting them. These are the ideal areas for added redundancy to disperse responsibilities and improve *DoSO*.

TABLE I: Shannon Index (H) and Evenness (E) for the normal, DS1, and DS2 scenarios for both topologies.

Topology	Scenario	H	E
Ecology Average	-	4.38	1.27
Relay to Control Center	Normal	4.76	1.52
-	DS1	4.75	1.52
-	DS2	4.31	1.38
Control Center to Relay	Normal	4.86	1.57
-	DS1	4.85	1.55
-	DS2	4.00	1.28

Shannon Index (H) and Evenness (E) in Table I can also help to identify the level of diversity in the system. While food webs have an average H of 4.38, the *Control Center-to-Relay* topology is slightly lower at 4.00. This lower value indicates that the network lacks species richness in DS2. This is most likely due to the uneven distribution of devices as a result of the disturbance scenario. At first glance, E further supports this conclusion. However, an E of a species when normalized is almost always from 0 to 1. Although the ecological average is 1.27 which is also higher than expected any value higher than ecology is highly unlikely. When computed for all case studies, E, within the context of this study may prove to be

unreliable for inter-cyber modeling. However, *H* still assists us with the conclusion that the traditional topology structure in place for cyber systems in the WSCC 9-bus topology lacks redundancy and support from nearby devices. This can be seen in both topologies for the normal scenario or where *H* exceeds the ecology average. However, in both DS2 scenarios *H* falls below the ecological average. This change indicates a lack of balance and integrated network structure.

B. Topology Metrics

Traditional topology metrics (average node degree, ND, average clustering coefficient, CC, and average betweenness centrality, BC) were also applied to the cyber case studies to understand the network node dependencies.

TABLE II: Topology Evaluation Results of Normal, DS1, and DS2.

Topology	Scenario	ND	CC	BC
Relay to Control Center	Normal	2.19	0.024	0.70
-	DS1	2.00	0.027	0.63
-	DS2	1.65	0.016	0.049
Control Center to Relay	Normal	2.10	0.024	0.70
-	DS1	2.00	0.027	0.038
-	DS2	1.22	0.024	0.038

The results from Table II indicate that the more densely connected nodes are found in both case studies' normal scenarios. The *BC* decreases significantly in Disturbance 2 for both topologies. This suggests that the network structure has lost key nodes through which critical information passes. The *ND* similarly decreases for all the disturbances. The largest loss is seen for Disturbance 2 (*Control Center-to-Relay*), affirming the criticality of a system lacking redundancy. At edge nodes in a graph, there is a possibility of higher disturbance in lower level network devices like relays. Lastly, *CC* matches well with the ecological results in the previous paragraphs where the network (*WoV*) gains strength from the loss of an end-of-topology node in DS1.

C. Performance Goals

Disturbance scenarios can lead to a diverse range of impacts in cyber networks. Specifically, in the case of Disturbance 1, relays 13 and 20 confront a Denial-of-Service (DoS) attack. This attack not only disrupts the functionality of the targeted relays but also causes a ripple effect on associated components. The local *HMI* and control center *HMI* are adversely affected due to their incapability to communicate to the specific relays. On the other hand, in the case of Disturbance 2 where the communication between Relay 3 to Substation A's SW1, Substation's SW 0, and router 0 are facing a DoS attack, the disruption affects more network of components. As can be seen from Fig. 1, router 0 stands as the pivotal connection hub, interlinking all routers, and is responsible for the aggregation of both data and commands. As a consequence, Disturbance 2 influences all the connected actors in the cyber network.

Performance Percentage (PP, Eq. 6) is here defined as the ratio of output packets in different cases and the total output packets in normal conditions to better quantify the performance. The affected components and performance evaluation are listed in Table III.

$$PP = \left(1 - \frac{\#Missing\ packets}{\#Total\ packets_{normal}}\right) \times 100\% \qquad (6)$$

TABLE III: Performance evaluation (components impacted and PP) for the two disturbance scenarios tested.

Scenarios		Impact	PP
Disturbance 1	Relay to Control Center Control Center to Relay	R13, R20, SubA_HMI, CC_HMI	90%
Disturbance 2	Relay to Control Center Control Center to Relay	Relay and actors in SubA, r0-r3, CC_SW, CC_HMI	33%

The PP in disturbance 1 is 90% while it is 33% in disturbance 2 scenarios suggesting the disturbance 2 scenario caused more packet loss. Comparing this with the earlier results, it coincides well with topology metrics but is inverse from the *WoV* predictions. This indicates that system performance is lacking substantially, but the overall topology design itself after the disturbance is more resilient. Therefore it can be concluded that creating a more interconnected cyber communication topology is possible via the integration of backup substations and routers that can continue to deliver data even when the primary device is no longer operable.

V. Conclusion

In this work a cyber communication topology is explored for the WSCC 9-bus system, employing ecological analysis methods that have been related to resilience and sustainability, in addition to traditional topological metrics. These scenarios revealed the lack of redundancy in the normal topology for both sending and receiving communications. The results conclude that a secure information flow network would optimally include several redundant devices including one at the main control center in the network.

Overall, our findings are summarized as:

- Ecological Network Analysis for the WSCC 9-bus system is effective in identifying topologies more susceptible to disturbances in the inter-cyber interdependencies.
- Topology metrics and Ecological resilience metrics support the need for a more redundant topology where devices have support from many connected components.
- All results support the need for a higher amount of devices dedicated to the support of primary existing devices in the system specifically at the control and substation areas.

The topology developed in this work can be applied to other power system case studies for further analysis of overall system resiliency among a higher device diversity network. Identifying patterns in additional power grid case studies will

help to quantify a Widow of Vitality range suitable for power grid systems. Possible challenges include retaining the same disturbance scenarios with the growth of network size in new case studies. Specifically, the addition of multiple two-way topologies of information flow will be explored utilizing the same metrics.

The fundamental goal of this work revolves around enhancing the robustness of the power grid. Grounding the approach in real-world feasibility and ensuring that it remains accessible and user-friendly for decision-makers is critical.

VI. Acknowledgements

The authors would like to thank Aisling Gilmore for her assistance in this work and the members of Sandia Laboratory Directed Research and Development Project #229324 for their collaborative discussion. This work was funded by Sandia National Laboratory.

References

[1] F. Li, X. Yan, Y. Xie, Z. Sang, and X. Yuan, "A review of cyber-attack methods in cyber-physical power system," in *2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP)*, 2019, pp. 1335–1339.

[2] S. Katsikeas, P. Johnson, M. Ekstedt, and R. Lagerström, "Research communities in cyber security: A comprehensive literature review," *Computer Science Review*, vol. 42, p. 100431, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S157401372100071X

[3] Computer Weekly, "Ukraine cyber teams responded to more than 2000 attacks in 2022," 2022. [Online]. Available: https://www.computerweekly.com/news/252529292/Ukraine-cyber-teams-responded-to-more-than-2000-attacks-in-2022

[4] J. Giri, "Real-time grid management: Keeping the lights on!" *IEEE Power and Energy Magazine*, vol. 21, no. 3, pp. 51–60, 2023.

[5] NERC and the six Regional Entities, "Ero enterprise publishes cyber-informed transmission planning white paper," North American Electric Reliability Corporation, Tech. Rep., May 2023.

[6] "Multiyear plan for energy sector cybersecurity," Department of Energy, Office of Electricity Delivery and Energy Reliability, Tech. Rep., Mar. 2018. [Online]. Available: https://www.energy.gov/ceser/articles/doe-multiyear-plan-energy-cybersecurity

[7] R. Ulanowicz, S. Goerner, B. Lietaer, and M. Gomez Bardon, "Quantifying sustainability: Resilience, efficiency and the return of information theory," *Ecological Complexity*, vol. 6, pp. 27–36, 03 2009.

[8] A. Chatterjee and A. Layton, "Mimicking nature for resilient resource and infrastructure network design," *Reliability Engineering & System Safety*, vol. 204, p. 107142, 2020.

[9] A. Chatterjee, R. Malak, and A. Layton, "Exploring system of systems resilience versus affordability trade-space using a bio-inspired metric," *Journal of Computing and Information Science in Engineering*, vol. 21, no. 5, 2021.

[10] T. Dave and A. Layton, "Designing ecologically-inspired robustness into a water distribution network," *Journal of Cleaner Production*, vol. 254, p. 120057, 2020.

[11] H. Huang, Z. Mao, V. Panyam, A. Layton, and K. R. Davis, "Ecological robustness-oriented grid network design for resilience against multiple hazard," *IEEE Transactions on Power Systems*, pp. 1–13, 2023.

[12] V. Panyam, H. Huang, K. Davis, and A. Layton, "Bio-inspired design for robust power grid networks," *Applied Energy*, vol. 251, p. 113349, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306261919310232

[13] H. Huang, Z. Mao, V. Panyam, A. Layton, and K. R. Davis, "An ecological robustness-oriented approach for power system network expansion," *ArXiv*, vol. abs/2107.06178, 2021.

[14] A. Chatterjee, H. Huang, A. Layton, and K. Davis, "A multigraph modeling approach to enable ecological network analysis of cyber physical power networks," in *2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2021.

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

[16] S. Sun, E. Payne, A. Layton, K. Davis, S. Hossain-McKenzie, and N. Jacobs, "Bio-inspired and ai deepwalk based approach to understand cyber-physical interdependencies of power grid infrastructure," in *IEEE 55th North American Power Symposium (NAPS)*, Oct 2023.

[17] R. E. Ulanowicz, "Quantitative methods for ecological network analysis," *Computational Biology and Chemistry*, vol. 28, no. 5, pp. 321–339, 2004. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1476927104000647

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

[19] A. S. Al-Hinai, *Voltage collapse prediction for interconnected power systems*. West Virginia University, 2000.

[20] B. Bollobás, *Modern graph theory*. Springer Science & Business Media, 1998, vol. 184.

[21] E. W. Zegura, K. L. Calvert, and M. J. Donahoo, "A quantitative comparison of graph-based models for internet topology," *IEEE/ACM Transactions on networking*, vol. 5, no. 6, pp. 770–783, 1997.

[22] S. Hossain-McKenzie, N. Jacobs, A. Summers, R. Adams, A. Chatterjee, A. Layton, K. Davis, and H. Huang, "Towards the characterization of cyber-physical system interdependencies in the electric grid," 2023.

[23] R. E. Ulanowicz, *Growth and development: ecosystems phenomenology*. Springer Science & Business Media, 2012.

[24] R. Margalef, "Information theory in ecology," 1973.

[25] R. E. Ulanowicz, "Information theory in ecology," *Computers & chemistry*, vol. 25, no. 4, pp. 393–399, 2001.

[26] B. D. Fath, "Quantifying economic and ecological sustainability," *Ocean & Coastal Management*, vol. 108, pp. 13–19, 2015.

[27] A. Chao and T.-J. Shen, "Nonparametric estimation of shannon's index of diversity when there are unseen species in sample," *Environmental and ecological statistics*, vol. 10, pp. 429–443, 2003.

[28] I. Nijs and J. Roy, "How important are species richness, species evenness and interspecific differences to productivity? a mathematical model," *Oikos*, vol. 88, no. 1, pp. 57–66, 2000.

[29] J. A. Camargo, "On measuring species evenness and other associated parameters of community structure," *Oikos*, pp. 538–542, 1995.

[30] C. P. Mulder, E. Bazeley-White, P. G. Dimitrakopoulos, A. Hector, M. Scherer-Lorenzen, and B. Schmid, "Species evenness and productivity in experimental plant communities," *Oikos*, vol. 107, no. 1, pp. 50–63, 2004.

[31] T. M. DeJong, "A comparison of three diversity indices based on their components of richness and evenness," *Oikos*, pp. 222–227, 1975.