Bio-inspired and AI DeepWalk Based Approach to Understand Cyber-Physical Interdependencies of Power Grid Infrastructure

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

2023 North American Power Symposium (NAPS) | 979-8-3503-1509-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/NAPS58826.2023.10318688

Abstract—**The occurrence of cyber and physical disturbances in power systems is increasing, leading to increased public focus on cyber-physical architectures. It has been observed that disturbances can propagate between cyber and physical systems, highlighting the need to study their interdependencies. In this paper, we present an approach to improve the characterization of cyber-physical interdependencies through modeling techniques. These improved assessments of dependencies can then help optimize system design to improve functional resilience. To achieve this goal, we transform the cyber-physical architecture into a graph and apply bio-inspired network analysis using bipartite network methods to characterize the system during disturbances. Moreover, we apply a DeepWalk-based method to cluster the components based on their interdependencies. A WSCC-9 bus system is used for numerical study and quantification.**

Index Terms—**bipartite network, cyber-physical interdependencies, cyber attack, DeepWalk method, power grid resilience**

I. Introduction

Modern technologies have made power systems more intelligent yet more vulnerable to attacks. The adoption of new technologies is rapidly increasing, offering more opportunities for cyber attacks to occur. Well-known cyber attacks include Denial-of-Service (DoS), Man-in-the-Middle (MiTM) [1] and malware attacks [2]. Recently, the Ukrainian Computer Emergency Response Team (CERT) [3] reported their energy infrastructure monitoring system being repeatedly targeted, highlighting the ability of cyber disturbances to influence physical components and cause blackouts. Dealing with such threats requires treating cyber-physical systems comprehensively to understand the role that interdependencies play during disturbances.

Bio-inspired network design shows unconventional routes toward achieving traditional resilience goals. Beyond power grids, applications have included engineering makerspaces [4], water distribution networks [5], and industrial resource networks [6], [7]. Previous results stemming from the use of *ecological modeling and analysis techniques* [8] for power grid resilience, propose the use of modularity analyses on bipartite network models to understand the role of cyber-physical interdependencies in the resilience of complex cyber-physical system of systems. A modularity analysis supports investigations into network partitioning since modularity identifies actor groupings based on their interactions. It can also identify things like hub actors, which highly connect the network, and specialized actors, which are at risk of easily being disconnected from the rest of the network.

Examples of bipartite networks include neural networks, transportation centers, and mutualistic ecosystems like plant-pollinator networks [9], [10]. A modularity analysis is then able to identify critical actors in the system, a technique commonly used by ecologists for conservation efforts [11], [12]. This paper looks explicitly into mutualistic networks like plant-pollinator networks, due to their resistance to disturbances and mutually beneficial interactions. Modularity, in conjunction with nestedness and connectedness, helps to model the interactions between the cyber and physical components of a power system and reveals trends between a power system's resilience (based on contingency analyses) and its interconnectivity.

Similarly, clustering techniques are used in physical power systems research for interconnected analysis. Different clustering methods previously found a power system's load pockets [13]. Risk assessment, anomaly detection, and intrusion detection are a few examples of utilizing clustering [2]. In [14], the authors propose studying the state of a cyber-physical system after attacks by isolating the affected vertices and grouping them as a single cluster. The work in this paper explores the possibility that classification by vertices' could help better understand data flow and risk propagation within systems.

The motivation for this work is to explore diverse methods for identifying cyber and physical interactions in power grid networks.

This paper's contributions include:

1) Applying novel bipartite network methods to analyze cyber-physical interdependencies.
2) Applying DeepWalk and other AI methods to cluster the components and analyze the interdependencies.
3) Analyzing the cyber-physical disturbances scenarios by utilizing a DeepWalk method for risk assessment.

S. Sun, E. Payne, A. Layton, K. Davis are with Texas A&M University, College Station, TX. S. Hossain-McKenzie, N. Jacobs are with Sandia National Laboratory. This work was supported by the Sandia Laboratory Directed Research and Development Project #229324.

The remaining paper proceeds as follows: Section II provides an overview of our case study, Section III describes our methods in detail, followed by a discussion of the results in Section IV, and a conclusion in Section V.

II. Background and Problem Formulation

Numerous structural imbalances can present challenges to power system security [1]. As [15] illustrated, the power outage was caused by the adversary placing malware in the communication system and opening the target circuit breakers. DoS can result in a component failing to provide service, causing an unscheduled power outage resulting from communication disruptions [1]. Malware attacks could cause configuration problems, communication devices impacted, sending hazardous remote control, etc. [15].

Prior applied Ecological Network Analysis (ENA) shows the normal operation of the WSCC 9-bus power system's synthetic cyber network presents a less cyclical nature than food webs [8]. A look at the ratio of specialized consumers to producers, known as the specialized predator ratio, is seen to be high for the power network, indicating that power system components have a high dependency on each other and there is less redundancy in the overall network [8].

In this paper, we continued working on disturbances scenarios of cyber-physical systems to aid in nodal clustering methods to understand the characterization of CPS and how information flows within and between different clusters [8], [16].

An augmented WSCC-9 bus system is used for the case study, where the physical system is composed of 3 generators (G), 9 buses (B), and 3 loads (L) [17]. Based on the structural data, we have separated the infrastructure into three individual substations. Fig. 1 shows the one-line diagram for the WSCC-9 bus physical system; for better illustration, different substations are color coded.

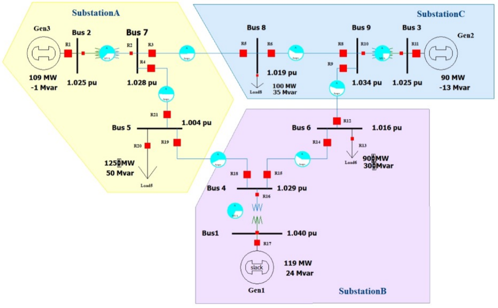

Fig. 1: One-line Diagram for WSCC-9 Bus Physical System by 3 Areas

As indicated in fig. 2, a cyber system is generated based on 3 different substations, comprised of relays (R), Ethernet Switches (ES), human-machine interfaces (HMI), routers (r), and firewalls (FW). The cyber system monitors and transfers real-time data and sends commands that control the physical components. Relays, as defined as cyber-physical components, become the linkage between the physical and cyber networks of the WSCC-9 bus case study.

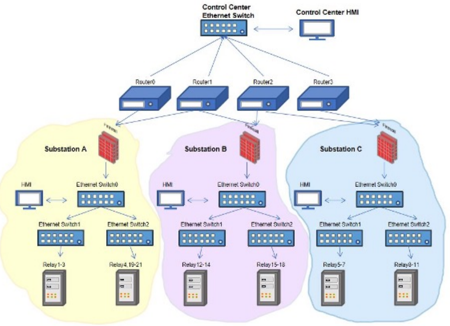

Fig. 2: Cyber Network for WSCC-9 Bus Physical System by 3 Areas

The following methods are pursued in this paper.

1) Fully Functioning Network Analysis via Bipartite Network: Structural information on cyber-physical connections help formulate answers on critical nodes and community groupings.

- Bipartite Network visualization: module formation and out-of-node groupings from a fully functioning network
- Quantitative information: Nestedness, Connectivity, and Modularity regarding a fully functioning network

2) Risk Assessment of N-1 Disturbance Scenarios via Cluster-based approach towards cyber-physical interdependency analysis: We assumed DoS occurred to physical components and cyber components. One component whether physical or cyber is in a state of failure which gives us an *N-1* state for the system. We assess the risks of the structure and guess the most probable location of the next attack. Several scenarios are assumed as followed:

- DoS of physical components: generator 1 outage and branch 6-9
- DoS of cyber components: substation C router 3
- Cyber-physical disturbance: a combination of physical disturbance and cyber disturbance

During the malware attack, one device is targeted and then the error propagates through the system. In this paper, we are interested in knowing whether a DeepWalk-based detection method could explore the interdependencies of each community.

III. Methodology

A. Ecological Bipartite Modeling and Analysis

Previous bio-inspired design work using ENA explored graph visualization and matrix-based depictions to capture interactions between actors in a network [8]. The NxN structural matrix, where N is the number of actors or nodes inside your system boundaries, creates quantitative characteristics from the network. The model uses graph-theory-based methods to quantify the characteristics of the system.

Using a bipartite network depiction (Fig. 3) enables the use of a modularity analysis to understand the interaction modules in the network. The modularity level of a bipartite network is limited by the total number of interactions possible vs. actualized in a network. Connectivity (C, (2)) is thus important to a modularity analysis and measures a system's complexity. Generally, the lower the connectivity the higher the modularity. Connectivity alone cannot determine network stability, but it does help us understand the modularity of the network since it controls the level of modularity achievable.

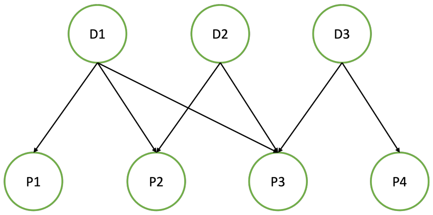

Fig. 3: A Bipartite Network shown as two groups of actors ”D” indicating digital components and ”P” indicating physical components.

Using the WSCC-9 bus model as our network of interest, a bipartite interaction matrix is constructed and ecologly metrics are analyzed. Modularity (Qb, (1)) calculates the overall network modularity, where E is the total number of interactions in the network. E_{ij} is the matrix entries where one represents an edge or zero for none [4], [18]. Where g_i and h_j are the module indices of the nodes i and j, and k_i and d_j represent the degrees of i and j. Delta (δ) parses the module indices for pairings between actor groups. In this case being cyber and physical power grid components and then assigns a value of one if they are in the same module and a value of zero if they are in two different modules. This process is recursive and is carried out initially by dividing the network into two modules and calculating the modularity. This continues until the network has reached maximum modularity [19], [20].

$$Qb = \frac{1}{E}\sum_{ij}(E_{ij} - \frac{k_i d_j}{L})\delta(g_i, h_j) \tag{1}$$

Connectivity indicates there are identifiable bounds that depend on the network size of N rows and N columns [4], [18], [21], [22]. Here L is the sum of all the edges or links and N squared represents the total number of possible connections. A connectivity of one means that all possible interactions are occurring and every element is connected to each other. A connectivity of zero indicates there are no interactions in the network.

$$C = \frac{L}{N^2} \tag{2}$$

Nestedness is another ecology metric prominent in plant-pollinator studies. This metric helps to investigate two groups of modules interacting across their respective modules [23], [24]. Further investigations of this metric include studying the stability of bipartite networks to disturbances and analyzing failure rates of large-scale industrial networks [25]. Nestedness is a quantity detailing the structural hierarchy of the overall network [22], [26]. Highly nested networks observed by ecologists, calculated by *Nestedness based on Overlap and Decreasing Fill* (NODF, (4)), help to understand the resilience to disturbances [27]. The overall nestedness ranges from values of 0 to 100 or from 0 to 1 if the values have been normalized. Higher values indicate more nested networks similar to nature [28]. NODF continually compares the existing column value during the calculation to other column values (4). When the decreasing fill condition becomes met, either the first or second pair of interactions are less than the other. When this occurs the lower pair of interactions are represented by a zero in the calculation. Analyzing a network's nestedness is valuable because it creates more information about the interactions of that network in a diverse environment.

$$M_{ij} = \begin{cases} 0 & ifc \leq k_j \\ \frac{n_{ij}}{min(k_i,k_j)} & otherwise \end{cases}. \tag{3}$$

$$NODF = \frac{\sum_{ij} M_{ij}row + \sum_{ij} M_{ij}col}{\frac{m(m-1)}{2} + \frac{n(n-1)}{2}}. \tag{4}$$

In (3), k_i is the sum of the row or column i, likewise, k_j, is the sum of the row or column j. Meanwhile, n_{ij} is the total number of entries matching between the two viewed values, and c is the number of entries that are a value of 1 for all values in k_j. In (4), NODF is the normalized value for the matrix to compare various matrix sizes together and produces the final NODF value from 0 to 1.

Bipartite models and a modularity analysis can provide quantitative values of the interactions between CPS regarding the reliability, serviceability, and sustainability of the network.

B. Interdependencies analysis by AI methods

The transmission of data on the cyber side of the power system sends commands and transmits real-time data. Since a cyber-physical system is composed of multiple layers, data has different paths and sequences. An attack could start by targeting one component, and then proceed to destroy the most costly device along the sequence.

The DeepWalk method can extract the information from a given graph as input. Millions of random walks are generated to extract the structure of a target vertex. By seeking the possibilities of learning interdependencies of a vertex by capturing neighborhood similarities and using skip-gram method to encode the interdependencies in a R^d vector, the training result could be used as risk analysis to presume the components most likely to be attacked next [29].

Meanwhile, Principal Component Analysis (PCA) and k-means method could be utilized to reduce the latent variables to 2D space and find clusters containing both cyber and physical components.

The methodologies during the training session are described as followed:

1) Utilizing graph representation: Inspired by ecological modeling, a graph representation of the cyber-physical network could be generated as shown in Fig. 4. For better visualization, different colors are denoting different types of components in the cyber-physical system. In a more numerical way, let *G = (V,E)*, where each node (*V*) represents an actor (component); The edge (*E*) represents for the connections of actors (components).

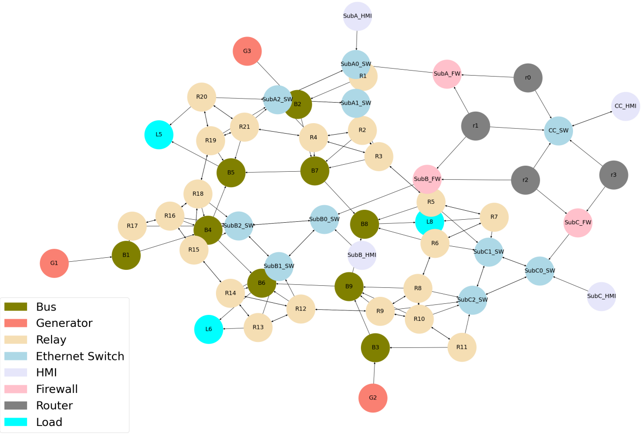

Fig. 4: WCSS-9 Cyber-physical Graph Representation

2) Applying DeepWalk methods for risk assessment and getting latent variables: Deepwalk method is an unsupervised deep learning method on graphs [29]. It is a statistical model that learns probabilities from the data of randomly generated walking sequences. For example, a randomly formed sequence rooting from *'G1'* within eight steps, could be indicated as $W_{v_i}^1 = \{G1 \rightarrow B1 \rightarrow R17 \rightarrow SubB2\_SW \rightarrow SubB0\_SW \rightarrow SubB\_FW \rightarrow r2 \rightarrow CC\_SW\}$.

The estimated likelihood is utilized as an equation for the starting vertex v_i can be denoted as: $Pr(v_i|(v_1, v_2, ..., v_{i-1}))$. In order to get the latent variables, a mapping function: $\Phi : v \in V \mapsto \mathbb{R}^{|V| \times d}$ is introduced, by which the interdependencies could be represented as a R^d vector. Hence, the likelihood is estimated by:

$$\Pr(v_i|(\Phi(v_1), \Phi(v_2), ..., \Phi(v_{i-1}))) \tag{5}$$

Equation (5) yields an optimization problem:

$$\underset{\Phi}{\min.} - \log \Pr(\{v_{i-w}, v_{i-1}, v_{i+1}, ..., v_{i+w}\})|\Phi(v_i)) \tag{6}$$

The algorithm contains a random walk generator and an update loop where a random walk will take the random sequence of nodes W_{v_i} within a given walk length *t*. By giving the iteration number γ, the algorithm will generate a random walk, and a skip-gram algorithm is utilized to fulfill (6).

Skip-gram is an unsupervised deep learning method, using the target node to predict the related vertices. In this algorithm, hierarchical softmax is built to summarize the conditional probability by assigning the vertices to be the leaves of a binary tree. Given that $u_k \in V$, leaves of the tree could denote as (b_0,b_1,...,$b_{\lceil log|V|\rceil}$), where b_0 is the root of the tree and $b_{\lceil log|V|\rceil}$ equals to u_k. The conditional probability of being attacked next transforms into searching the maximum probability of a particular path in a hierarchical tree [29]. Then the conditional probabilities for given target node v_j could be calculated as:

$$\Pr(u_k|\Phi(v_j)) = \prod_{l=1}^{\lceil log|V|\rceil} \Pr(b_l|\Phi(v_j)) \tag{7}$$

Based on the DeepWalk method, latent variables embedded in the interdependencies could be generated for each vertex. Due to the fact that each embedded vector is in *d* dimension. We need other AI methods to encode the vectors to 2D for better understanding and visualization.

3) Utilizing Principal Component Analysis (PCA) and k-means methods for clustering : PCA is a widely used algorithm for reducing the dimensionality of data points by transforming latent vectors into a linear combination of the original data points and reflecting the same information [30]. Utilizing PCA Analysis reduces the dimension of the latent vectors could to 2D [30]. K-means algorithm clusters the data points by the nearest centroids [31].

IV. Result and Discussion

A. Ecology Metrics

Modularity and connectance of the cyber-physical system, coupled with contingency analyses, provide critical information about the design of cyber-physical interconnections and a grid's resilience. Table I shows the analysis results.

TABLE I: Bipartite Modularity Analysis Results

Metric	Bipartite Network Model
Connectance	0.034
Nestedness	0.002
Modularity	0.890

The bipartite results indicate nodal groupings through defined ecological metrics in Section III. The bipartite model has a low connectivity value of 0.034, indicating that preliminary cyber-physical connections have a very low percentage in the overall network. A low nestedness value (0.002) also indicates a short range/lower ability to create inter-node influence within the network. This could be an effect of the low diversification between cyber-physical connection types and appearances. Lastly, modularity (0.890) indicates that the power grid structure is heavily influenced by the original physical network due to distinct, densely-connected groupings of subsystems. In this case, the subsystems can be equated to power grid substations or micro-grids.

Fig. 5 helps to visualize the nature of the bipartite connections. The colors represent the defined modules, black lines indicate out-of-module connections, and no lines mean there are no interconnections captured for those nodes. Fig. 5 for example shows a module as B7, R2, R3, and R4, while B2 has an inter-module connection with R1 and an out-of-module connection with R13.

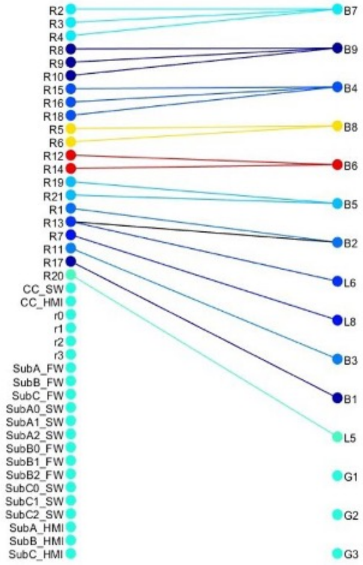

Fig. 5: Bipartite Cyber-physical Model, with Different Colors Indicating Each Module.

B. Risk Assessment and Community Detection

A graph representation of WSCC-9 cyber-physical system, manifesting in Fig. 4, is used as an input in this case study. There are a total of 57 components in the cyber-physical system. The average number of vertices for data transfer and command sent from the start node to the end node is approximately 8, hence the walk length *t* is set to be 8. The window size *w* is assigned as 3 (based on previous works [8]) and the embedding size *d* as 256. This is a proper vector space for all methodologies. We assume the learning rate to be 0.01 based on previous works [8].

1) Risk assessment: We are seeking the adversary's next step during the disturbance scenarios assuming that the adversary will commonly target one component and keep the attack proliferating. In this case study, we assume several *N-1* disturbance scenarios including physical and cyber components. The probability of each node being attacked next is calculated by eq.5. We ranked the eight components which are most likely to be attacked next in the event of the *N-1* disturbance. After training the skip-gram model, the result is shown in table II.

TABLE II: Components with High Risks During Disturbance

Components facing DoS		**High Risks Components Related**
Physical Components	G1	{B1,B4,L5,R15-R20,SubB2_SW}
	B6	{B3,G2,B3,R9,R11,R12-R15}
	B7	{B2,G3,L8,R1-R4,SubA1_SW}
	B8	{G2,B3,L8,R3,R7,R8,R10,R11}
	B9	{G2,B3,L8,R7,R8,R10, R11,SubC2_SW}
Cyber Components	Router 3	{r0-r2,SubA_FW-SubC_FW, CC_SW,CC_HMI}

Table II reveals the devices at a high-risk level related to the components attacked already. Suppose Generator 1 ($G1$) is facing the DoS attack, the result shows Bus 1 ($B1$), Bus 4 ($B4$), Load 5 ($L5$), Relay 15 to 20 ($R15-20$), Substation B's switch ($SubB2\_SW$) are the components most likely to be the next target. In comparing this to the original network the result with the physical and cyber network is shown in Section II. $G1$, $B1$, and $B4$ are connected with $G1$; $R15-R20$ are protecting the buses and lines within substation B; $SubB2\_SW$ is the Ethernet switch to monitor and transfer data for $G1$ and related buses. By inspection, all the components in high risks are highly associated with $G1$. We then compared the rest of the circumstances, all the results are in consistent with the cyber-physical network.

This is an important finding in risk mitigation. During the disturbance scenario, DoS of one component, physical or cyber, could result in failure of other pinpoints with high risks and cause severe problem. If the system operators could estimate which component is most likely to be attacked next, we could start an action and mitigate the disturbance.

2) Clustering results: Employing a DeepWalk based algorithm, the result of is shown in Fig. 6. Taking $G1$ as an illustration, {G1,B1,B4,R15,R16,R17,SubB2_SW,R18,SubB_HMI} are in the identical cluster.

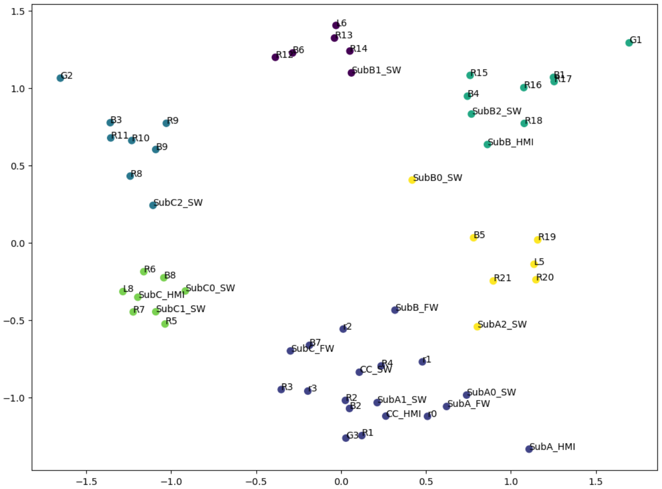

Fig. 6: Clusters Generated by DeepWalk Based Approach

Overall, our findings are summarized as:

- The algorithm shows that nodes in the same cluster are highly related. Most of the physical components in a cluster are physically located in the same substation. The clustering results for most network components are not restricted by physical area.

- Bipartite analysis support results of the clustering findings and show a dependence on the physical components.
- There are cyber components and physical components within one cluster, which proves that physical and cyber components are interpenetrating.
- The result implies that the nodes within the same cluster are more likely to get attacked simultaneously.

We believe our results cast a new light on cyber-physical interdependencies studies. Future systematic investigation for both methods will be conducted.

V. Conclusion

Advancements to analyze changes to cyber-physical power grids in diverse disturbance scenarios through bio-inspired clustering, and deep walk methods were explored in this work. The results indicate that bio-inspired methods including bipartite networks can provide valuable information regarding cyber-physical connections. Moreover, we provide convincing evidence for DeepWalk which delivers valuable risk assessment and community detection results.

Expanding to different case studies and identifying patterns and relevance of cyber components relative to physical networks will help to verify the results of this work. Possible challenges include applying transient modeling and analysis to our current methodologies. Further expansion of case studies with breadth and severity of disturbances will help assist to identify benchmarks. Our primary goal is to improve grid resiliency through interdependence analysis and risk mitigation. Respecting real-world feasibility as well as usability by decision-makers is a crucial component in the consideration of future infrastructure.

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] [Online]. Available: https://cert.gov.ua/articles

[4] S. Blair, H. Banks, J. Linsey, and A. Layton, “Bipartite network analysis utilizing survey data to determine student and tool interactions in a makerspace,” *2021 ASEE Virtual Annual Conference*. [Online]. Available: https://par.nsf.gov/biblio/10331810

[5] T. Dave and A. Layton, “Extending the use of bio-inspiration for water distribution networks to urban settings,” in *International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, vol. 83976. American Society of Mechanical Engineers, 2020, p. V008T08A001.

[6] A. Chatterjee, C. Brehm, and A. Layton, “Evaluating benefits of ecologically-inspired nested architectures for industrial symbiosis,” *Resources, Conservation and Recycling*, vol. 167, p. 105423, 2021.

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

[8] 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.

[9] C. F. Dormann, B. Gruber, and J. Fründ, “Introducing the bipartite package: analysing ecological networks,” *interaction*, vol. 1, no. 0.2413793, pp. 8–11, 2008.

[10] C. F. Dormann, J. Fründ, N. Blüthgen, and B. Gruber, “Indices, graphs and null models: analyzing bipartite ecological networks,” *The Open Ecology Journal*, vol. 2, no. 1, 2009.

[11] S. Watts, C. F. Dormann, A. M. Martín González, and J. Ollerton, “The influence of floral traits on specialization and modularity of plant–pollinator networks in a biodiversity hotspot in the peruvian andes,” *Annals of Botany*, vol. 118, no. 3, pp. 415–429, 2016.

[12] D. W. Carstensen, M. Sabatino, and L. P. C. Morellato, “Modularity, pollination systems, and interaction turnover in plant-pollinator networks across space,” *Ecology*, vol. 97, no. 5, pp. 1298–1306, 2016.

[13] K. M. Rogers and T. J. Overbye, “Clustering of power system data and its use in load pocket identification,” in *2011 44th Hawaii International Conference on System Sciences*, 2011, pp. 1–10.

[14] Z. Wang, L. Wang, H. Jiang, W. Huang, and J. Zhu, “Vulnerability analysis and evaluation of nodes in cyber-physical power system under the framework of blockchain,” in *2022 4th International Conference on Smart Power Internet Energy Systems (SPIES)*, 2022, pp. 2223–2228.

[15] M. Assante, T. Conway, and R. Lee, “Analysis of the cyber attack on the ukrainian power grid,” *SANS Industrial Control Systems Security Blog*, pp. 1–26, 2016.

[16] H. Huang, K. R. Davis, and H. V. Poor, “An extended model for ecological robustness to capture power system resilience,” 2023.

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

[18] S. B. G. H. Astrid Layton, Julie Linsey and H. Banks, “Modularity analysis of makerspaces to determine potential hubs and critical tools in the makerspace,” in *2022 ASEE Annual Conference & Exposition*. Minneapolis, MN: ASEE Conferences, August 2022, https://peer.asee.org/41476.

[19] M. E. Newman, “Modularity and community structure in networks,” *Proceedings of the national academy of sciences*, vol. 103, no. 23, pp. 8577–8582, 2006.

[20] C. O. Flores, T. Poisot, S. Valverde, and J. S. Weitz, “Bimat: a matlab package to facilitate the analysis of bipartite networks,” *Methods in Ecology and Evolution*, vol. 7, no. 1, pp. 127–132, 2016.

[21] M. A. Fortuna, D. B. Stouffer, J. M. Olesen, P. Jordano, D. Mouillot, B. R. Krasnov, R. Poulin, and J. Bascompte, “Nestedness versus modularity in ecological networks: two sides of the same coin?” *Journal of animal ecology*, pp. 811–817, 2010.

[22] A. James, J. W. Pitchford, and M. J. Plank, “Disentangling nestedness from models of ecological complexity,” *Nature*, vol. 487, no. 7406, pp. 227–230, 2012.

[23] A. Clifton and G. D. Webster, “An introduction to social network analysis for personality and social psychologists,” *Social Psychological and Personality Science*, vol. 8, no. 4, pp. 442–453, 2017.

[24] F. Senghore, E. Campos-Nanez, P. Fomin, and J. S. Wasek, “Using social network analysis to investigate the potential of innovation networks: Lessons learned from nasa’s international space apps challenge,” *Procedia Computer Science*, vol. 28, pp. 380–388, 2014.

[25] S. Bustos, C. Gomez, R. Hausmann, and C. A. Hidalgo, “The dynamics of nestedness predicts the evolution of industrial ecosystems,” *PloS one*, vol. 7, no. 11, p. e49393, 2012.

[26] W. Ulrich, M. Almeida-Neto, and N. J. Gotelli, “A consumer’s guide to nestedness analysis,” *Oikos*, vol. 118, no. 1, pp. 3–17, 2009.

[27] E. A. Martin, B. Feit, F. Requier, H. Friberg, and M. Jonsson, “Assessing the resilience of biodiversity-driven functions in agroecosystems under environmental change,” in *Advances in Ecological Research*. Elsevier, 2019, vol. 60, pp. 59–123.

[28] M. Almeida-Neto, P. Guimaraes, P. R. Guimaraes Jr, R. D. Loyola, and W. Ulrich, “A consistent metric for nestedness analysis in ecological systems: reconciling concept and measurement,” *Oikos*, vol. 117, no. 8, pp. 1227–1239, 2008.

[29] B. Perozzi, R. Al-Rfou, and S. Skiena, “Deepwalk: Online learning of social representations,” in *Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining*, 2014, pp. 701–710.

[30] A. Maćkiewicz and W. Ratajczak, “Principal components analysis (pca),” *Computers & Geosciences*, vol. 19, no. 3, pp. 303–342, 1993.

[31] M. Ahmed, R. Seraj, and S. M. S. Islam, “The k-means algorithm: A comprehensive survey and performance evaluation,” *Electronics*, vol. 9, no. 8, p. 1295, 2020.