2024 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT) | 979-8-3503-1360-4/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISGT59692.2024.10454149

Multimodal Learning in Cyber-Physical System: A Deep Dive with WSCC 9-Bus System

Khandaker Akramul Haque*, Katherine Davis
Texas A&M University
College Station, TX, USA
*akramwired@tamu.edu

Logan Blakely, Shamina Hossain-McKenzie,
Georgios Fragkos, Christopher Goes
Sandia National Laboratories
Albuquerque, NM, USA

***Abstract*—Multimodal learning has been utilized for numerous applications in cyber-physical power systems for load forecasting, voltage control and power quality monitoring. Although this learning technique has attained prominence in recent years, the use of this technique for predicting physical anomaly for cyber disruption is rather limited. This study uses the knowledge of t-distributed stochastic neighbor embedding (t-SNE) as a method widely used in multimodal learning for predicting the state of operation of a cyber-physical system. Naturally the aim of a power system is to keep the system operating which is termed as the normal or stable operating state of the power system. In the event of a possible contingency, the cyber-physical power system should foresee such event and can take preventive measures considering the comprehensive knowledge pertinent to this study. The Western System Coordinating Council (WSCC) 9-bus power system is taken as the test case for this study. In the event of loss of a generator, the system is brought into stable operation by load shedding. In the meantime, the system also underwent a Denial of Service (DOS) attack which denied the load shedding command. As a result, there was physical impact in the system which caused the system to become unstable. This is mitigated by issuing firewalls, which ensures the load shedding command will be initiated. Fusing cyber-physical data from multimodal relays and sensors located at strategic locations of the power system, the analysis is performed. The fused data is used to give an accurate estimation of the operating state that is visualized with t-SNE.**

***Index Terms*—embedding, cyber physical system, denial of service, load shedding**

I. Introduction

In the realm of ever-evolving landscape of cyber-physical systems (CPS), the integration of machine learning and optimization techniques has become increasingly crucial [1]. With the advent of renewable energy sources and their high penetration in modern power grids, accurate prediction and control are essential for grid reliability [2]. As a result, researchers and experts have turned their attention to multimodal learning, a field that consolidates data from various sensors and inputs to generate more robust inferences and insights [3]. This article explores the potential of multimodal learning in power systems, its benefits, scaling capabilities, and the opportunities it presents across various industries.

In this work, we consider the Western System Coordinating Council (WSCC) 9-bus power system as our testing environment which is emulated with a real-time digital simulator (RTDS) [4]. The description of this digital simulator is given in Section II. From this testing environment, we are collecting physical data from the relays and cyber data from the networking devices, leading to a multimodal analysis of the system. For the multimodal analysis of the system, dimensionality reduction is necessary since low dimensional data helps in data compression which is computationally efficient. This removes the dependence of redundant features which can holistically make simpler inference on the state of the system by plotting in a 2D space. Apart from the t-distributed stochastic neighbor embedding (t-SNE), principal component analysis (PCA), and random forest are some of the state-of-the-art techniques that are quite prominent for dimensionality reduction. Each of these techniques has some drawbacks of their own. PCA preserves the linear dependency of high dimensional data in low dimensional feature space and as result, it is not suitable for the non-linear feature space of a cyber-physical system. Random forest is dependent on decision trees which can overfit with much noise, and as a result, interpretation of the result becomes complex. Despite these drawbacks, transient analysis, voltage control and reliability analysis of power system have been done with PCA and random forest, but in every study they have used either only physical data or cyber data but not a combination of cyber-physical data [5].

In our work, we are considering the loss of generator 1 of the 9-bus system. As a result of this loss, the system becomes unstable, and to stabilize the system, load-shedding is initiated to loads connected at bus 5 and bus 6. This causes the system to become stable. In this instance, the power system is compromised with a cyber disruption where a denial of service (DOS) is initiated in the power system. Because of this disruption, the load-shedding command at bus 5 and bus 6 cannot be initiated. Finally, this disruption is mitigated by imposing firewall rules where normal communication is established and the load-shedding command is acknowledged

This article has been authored by an employee of National Technology & Engineering Solutions of Sandia, LLC under Contract No. DE-NA0003525 with the U.S. Department of Energy (DOE). The employee owns all right, title and interest in and to the article and is solely responsible for its contents. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this article or allow others to do so, for United States Government purposes. The DOE will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan https://www.energy.gov/downloads/doe-public-access-plan. This material is based upon work supported by the Sandia Laboratory Directed Research and Development Project # 229434.

979-8-3503-1360-4/24/$31.00 ©2024 IEEE

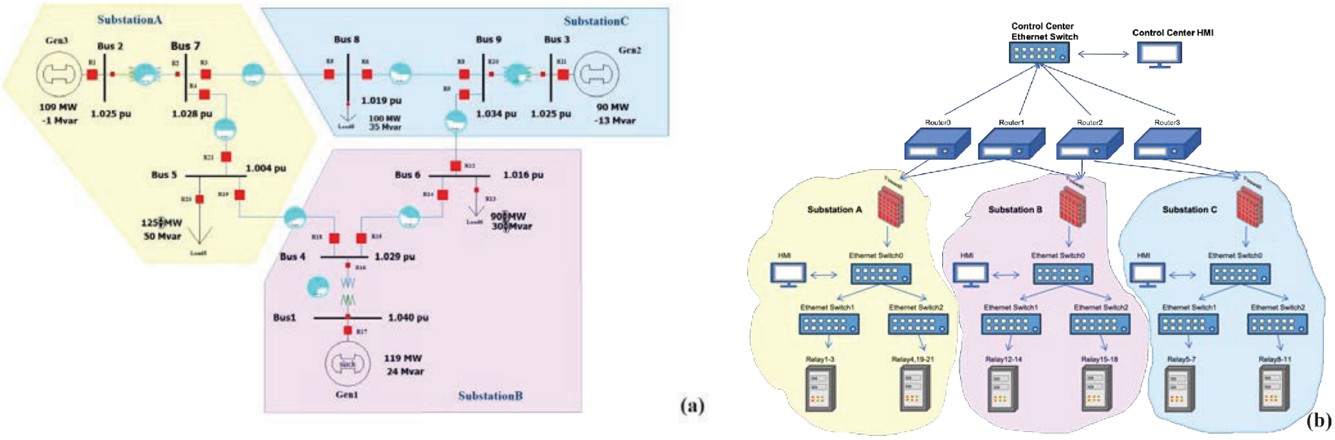

Fig. 1: Western System Coordinating Council (WSCC) 9-Bus Power System (a) Physical Topology, (b) Cyber Topology

by bus 5 and bus 6. Based on multimodal learning, a state of stable and unstable operating condition of the power system is finally predicted. Prior to our work, a similar approach has been used in prediction, but in that prediction dummy data was used unlike our work [6]. Thus, a dynamic risk assessment technique has been presented here that considers evolving cyber threats by combining cyber-physical analysis with real time data.

This paper is divided such that Section II introduces the testing environment, Section III details the algorithm used, Section IV presents the results of the multimodal learning, and Section V concludes the paper.

II. Testing Environment

For our testing environment, we are considering the WSCC 9-bus power system. It consists of 3 generators, 3 two-winding power transformers, 6 lines, and 3 loads. The environment is emulated with a real-time digital simulation (RTDS) [1], which allows the C37.118, a standard defining synchrophasors, frequency, and rate of change of frequency (ROCOF) measurement under all operating conditions [7], to stream data from the phasor measurement unit (PMU) to the RTDS WSCC 9-bus model and $SCEPTRE^{TM}$ which is a Sandia industrial control system (ICS) simulation tool that allows modeling and implementation of cybernetworks/control networks for process control systems [8]. Existing communication protocols such as Modbus and DNP3 are incorporated in $SCEPTRE^{TM}$.

Physical disturbance data sets were collected from 8 different PMUs in the WSCC 9-bus model. The cyber model violation data sets were collected that include the round trip time (RTT) of 3 different relays located in each substation A, substation B, and substation C. These features are given in Table I. A simplified approximation of the physical and cyber topology of the power system is given in Fig. 1. In this environment, two use cases are considered.

A. Baseline Scenario

First, the system begins in the steady state condition. Then, due to some disturbance, the generator connected to bus 1 is lost. Since the generator has tripped, the system is brought into steady state condition by using calculated load-shedding with the loads connected in bus 5 and bus 6 [1].

B. Use Case A: A DOS Prevents Special Protection Scheme (SPS)'s Load Shed

For the first use case, a Denial Of Service (DOS) attack is initiated on this particular synthetic power system which compromised the relays connected to bus 5 and bus 6. Hence, when the generator connected to bus 1 is lost, the load shedding command does not reach bus 5 and bus 6, which causes instability in the power system. The unstable nature of the system is reflected in the physical changes of frequency, voltage, and current. Moreover, the cyber entity such as the round trip time was also greatly affected. To represent the system holistically and to ensure reliability, analysis of the system is done by considering only the cyber entities, only the physical entities, and cyber-physical entities together. This is the unstable first scenario without any type of mitigation.

C. Use Case B: Mitigation of DOS

For the second use case, the DOS attack is circumvented with the help of firewalls and a mitigation technique. The load shedding is initiated to bring the system into stability. Those are further detailed in the results section.

III. Algorithm

The t-distributed Stochastic Neighbor Embedding (t-SNE) is used in the multimodal learning; it is commonly applied to high-dimensional data to visualize and explore patterns or clusters within the data [9].

t-SNE measures the pairwise similarities between data points in the high-dimensional space, X. It uses a Gaussian kernel to compute the similarities, where nearby points have

979-8-3503-1360-4/24/$31.00 ©2024 IEEE

TABLE I: Cyber and Physical Features

Cyber Features		
Feature Name	**Number of Features**	**Total**
Round Trip Time	2 per relay x 3 relays	6
Physical Features		
Feature Name	**Number of Features**	**Total**
Voltage Magnitude	3 per bus for 3 phase system x 8 bus	24
Voltage Angle	3 per bus for 3 phase system x 8 bus	24
Current Magnitude	3 per bus for 3 phase system x 8 bus	24
Current Angle	3 per bus for 3 phase system x 8 bus	24
Number of Samples		8999

higher similarity values. Suppose there are N high dimensional data X_1, X_1,..., X_N, a conditional probability P_{ji} proportional to the similarity between X_i, X_j using (1); where, σ_i represents the variance of X_i.

$$P_{ji} = \frac{exp(-||X_i - X_j\ ||^2/2\sigma_i^2\ )}{\sum_{k\neq i} exp(-||X_k - X_j\ ||^2/2\sigma_i^2\ )} \tag{1}$$

Similarly it constructs probability distributions, Q_{ji} based on pairwise similarities between data points in the lower-dimensional space, Y using (2) taking the variance of the Gaussian to be $1/\sqrt{2}$.

$$Q_{ji} = \frac{exp(-||X_i - X_j\ ||^2)}{\sum_{k\neq i} exp(-||X_k - X_j\ ||^2)} \tag{2}$$

To minimize P_{ji} and Q_{ji}, an optimization is reached with the Kullback-Leibler (KL) divergence between the probability distributions in the high-dimensional space, X and the low-dimensional space, Y. A cost function, K considering KL divergence is given in (3).

$$K = \sum_i KL(P_i||Q_i) = \sum_i \sum_j P_{ji} log \frac{P_{ji}}{Q_{ji}} \tag{3}$$

According to (3), P_i represents the conditional probability of high dimensional space, X. Each point of high dimensional data space has a different variance, σ. As a result the entropy, E associated with P_i has a proportional relation with σ. Stochastic Neighbor Embedding uses a concept called perplexity, $Perp$ and its mathematical relation with entropy, E is given in (4):

$$Perp(P_i) = 2^{E(P_i)} \tag{4}$$

The entropy, E of P_i is given in (5):

$$E(P_i) = \sum_j P_{ji} log_2 P_{ji} \tag{5}$$

The cost function, K given in (3), is minimized using the method of gradient descent. The simplified gradient formula of the cost function is given in (6):

$$\frac{\partial K}{\partial Y_i} = 4 \sum_j (P_{ji} - Q_{ji})(Y_j - Y_i)(1 + ||Y_i - Y_j||^2)^{-1} \tag{6}$$

The term $(Y_j - Y_i)$ in the gradient represents a spring between the points, (Y_j, Y_i). For positive value of the gradient, it would exert a compression force, and for negative value of the gradient, there would be a expansion force. The other terms, $(P_{ji} - Q_{ji}), (1 + ||Y_i - Y_j||^2)^{-1}$, represent the force exerted on Y_i by Y_j. The total force on Y_i is the summation of all the forces exerted on Y_i by all the other points in the embedding. Thus, the gradient in SNE is represented with the concept of attractive and repulsive force between the data points of low dimensional space Y_i and Y_j. This determines how the point moves in the embedding. The process is initialized with random Gaussian distribution with small variance. As a result in optimization process, to overcome the effect of local minima with gradient descent, a large momentum, m is used. The gradient update, G formula after the iteration t is given in 7 where l is the learning rate and m is the momentum.

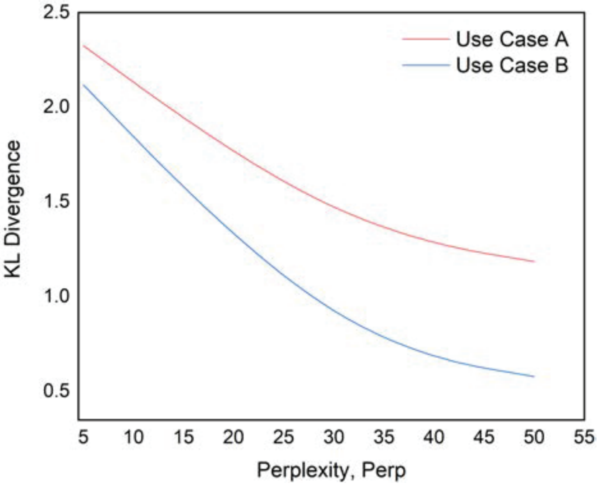

Fig. 2: Variation of KL Divergence with Perplexity

$$G^{(t)} = G^{(t-1)} + l\frac{\partial K}{\partial G} + m(t)(G^{(t-1)} - G^{(t-2)}) \tag{7}$$

In this work, we have used a fixed value of 30 for perplexity, $Perp$. To make the plot of t-SNE reproducible, PCA is used in the data preprocessing stage since the loss function associated with t-SNE can refer to a local minima with this initialization and can use this reference to generate similar plot. It needs to be mentioned that t-SNE becomes computationally expensive with the increase of sample size and the inference can become dependent on the data. The results of the work are given in the next section.

IV. Results

The sample data used in this work was taken from the synthetic grid of the WSCC 9-bus system. The features of interest are broadly divided into cyber features and physical features. Combining the cyber and physical features, a total of 102 features are taken into consideration.

From Table I, it can be seen that the dimensionality of the system is high, and it increases with the number of devices and quantities monitored in both cyber and physical layers. Eight of the nine buses in the WSCC 9-bus system have PMU devices installed. It is important to identify the most important features to include in the multimodal learning for efficiently detecting and monitoring the evolution of a cyber intrusion event's potential impacts on physical properties of the system. Such a high dimensional feature set with a large number of samples will not only increase the computation time but will also affect the ability of a machine learning model to express the underlying features clearly.

It should be mentioned that the cost function associated with t-SNE is inherently a non-convex function. As a result, there is every possibility the result might get stuck in a bad local minima. To overcome this, there is a method known as early

979-8-3503-1360-4/24/$31.00 ©2024 IEEE

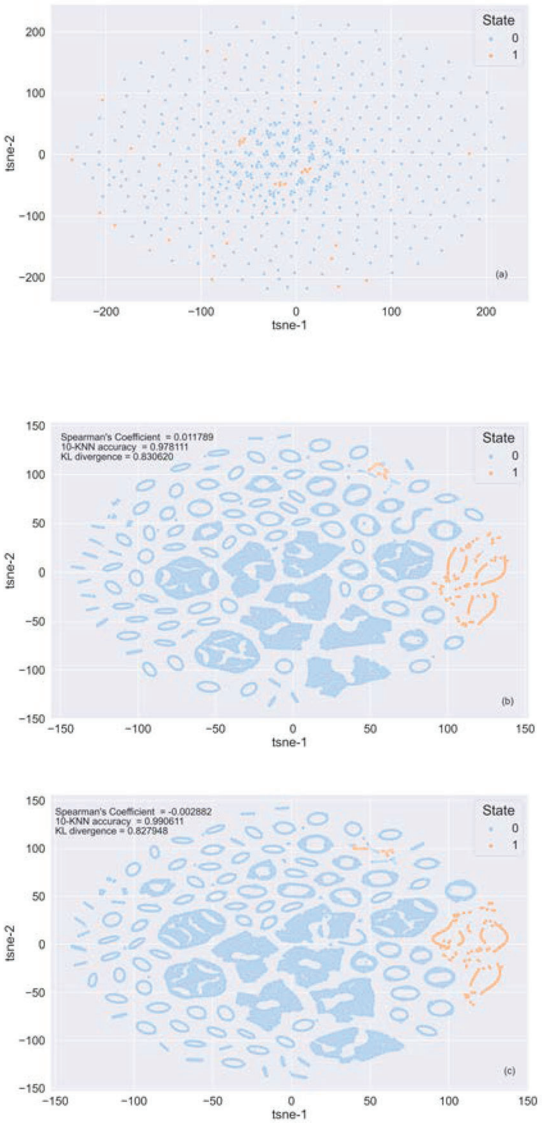

Fig. 3: Clustering of WSCC 9-Bus System with DOS Attack and No Mitigation (a) Cyber Features, (b) Physical Features, (c) Cyber-Physical Features

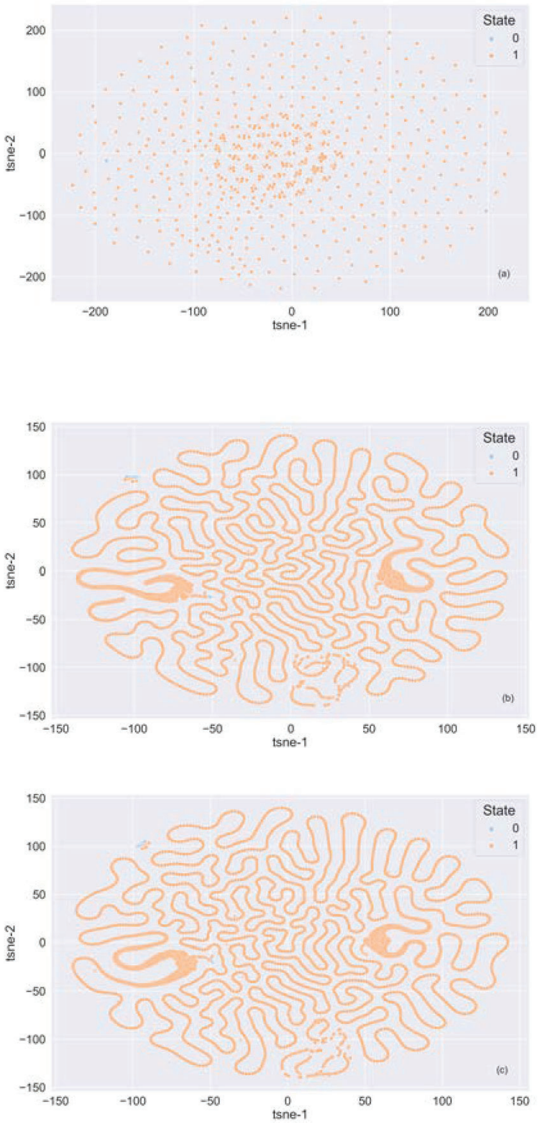

Fig. 4: Clustering of WSCC 9-Bus System with Mitigation after the DOS attack (a) Cyber Features, (b) Physical Features, (c) Cyber-Physical Features

exaggeration which momentarily multiplies a constant term with the probabilistic distances of all the points of the high dimensional space. In this study, for the first 250 iterations, early exaggerations is used.

As mentioned in Section III, we have taken a range of values from 5 to 50 as perplexity, $Perp$, for the visualization of the high dimensional feature space into a two dimensional plot. Although the value of KL divergence decreases with the increase of perplexity, it does not provide any additional information. In t-SNE, the concept of perplexity is related to the balance between attractive and repulsive forces. With a low value of perplexity, the attractive forces between the cluster is dominant, while on the other hand, with a high value of perplexity, the points in lower dimensional spaces are pushed further away. Thus, a high value of perplexity causes more separation in the cluster, resulting in the formation of sub-clusters. As a result, a value of 30 is taken as the optimized value for perplexity, $Perp$ [10]. This is shown in Fig. 2.

As described in Section II, two use cases are considered. For the first use case, a DoS attack is initiated which compromised the special protection scheme (SPS) in the test environment. The North American Electric Reliability Corporation (NERC) standard for frequency is used to distinguish between stable and unstable operation of the system [11]. Without any mitigation, the resulting visualization is shown in Fig. 3 in three ways: considering only the cyber features, only the physical features, and a combination of cyber-physical features. From the visualization of the cyber features in Fig. 3a, a single distinct cluster is dominant. Besides, when we shift our focus to Fig. 3b and Fig. 3c which considers only physical features and cyberphysical features combined respectively, it is interesting to note that there are several clusters. When a closer look is given at the combined cyber-physical graph of Fig. 3c, it appears that there are numerous clusters which are closer together around the center of the plot. These clusters represent the voltage magnitude, voltage angle, current magnitude and

979-8-3503-1360-4/24/$31.00 ©2024 IEEE

current angle of three phases. The rest of the clusters are the combined effect of round trip time and random noise in the system. During the stage of data preprocessing the covariance matrix of PCA initialization is considered. The covariance matrix shows that the t-SNE plot is dominated by phases of current and voltage magnitude. Besides, the t-SNE plot is less dominated by phases of current and voltage angles, and even less dominance is observed for round trip times when the same covariance matrix is considered. It is not clear which particular cluster represents which feature, but an inference can be reached, with the understanding of covariance matrix and t-SNE plot. The close together clusters are the combined effect of voltage magnitude, voltage angle, current magnitude and current angle of three phases and the more spread-out clusters are the combined effect of round-trip time and random noise in the system. Following this, when cyber-physical features are considered, the dominant clusters are close together in comparison with physical-only features. This phenomenon is mathematically related to Kullback–Leibler (KL) divergence. The lower the value of KL divergence, the closer are the similar clusters and dissimilar clusters. Besides, the Spearman's Correlation Coefficient is also calculated for physical and cyber-physical features. Positive value for this coefficient indicates that the distance of samples in the cluster will increase with sample size and negative value will indicate the opposite effect. Thus, similar clusters are closer together and so are the dissimilar clusters which effectively increases the separation between them in Fig. 3c. This phenomenon is further supported by 10-KNN accuracy where higher value is observed in Fig 3c [10]. Two color profiles are used to represent the operational state of the system. The orange color represents stable operation and the blue color represents unstable operation. The visualization accurately separates the stable and unstable clusters. On close observation, further inference can be made here. For unstable operation, we can find a distinct set of clusters and the color map coincides with these clusters, but for stable operation the color map is concentrated to the random noise. This can act as a first line of defense in detection, because for unstable operation distinct clusters can be observed. The separation between these clusters may be increased further by increasing the value of $Perp$, but for this study, a value of 30 for $Perp$ is high enough to distinctly separate the clusters.

For the second use case, a mitigation strategy is applied to the environment. The mitigation strategy is load-shedding. The visualization is shown in Fig. 4. As in the first use case, two color profiles are used, where orange represents a stable system and blue represents an unstable system. In this case, also the cyber-only features, physical-only features, and a combination of cyber-physical features are considered. Fig. 4a which considers the cyber-only features represents a single distinct cluster. Fig. 4b and Fig. 4c represent the stable system after the mitigation without any distinct cluster. It happens because after the mitigation strategy, the whole system behaves like a single system; this is distinctly unique from the initial unstable system which is shown in Fig 3.

The results produce some unique findings: (1) Combination of cyber and physical features produce better separation between the clusters in t-SNE. (2) t-SNE can be used to represent an unstable cyber-physical system.

V. Conclusion

The high dimensional feature space of the WSCC 9-bus sytem is modeled with t-SNE. 102 cyber-physical features are embedded in a two-dimensional plot to represent the unstable system under DOS attack. Results are further extended to represent a stable system after mitigation strategies. Although the WSCC 9-bus system is small, the features used in this study represent a cyber-physical system with a dataset substantial for multimodal learning. The learning outcome of this study could be used for studying large cyber-physical systems.

Acknowledgment

Special thank you to Adam Summers and Trupal Patel at Sandia National Laboratories for their help in setting up the testing environment.

References

[1] S. Hossain-McKenzie, N. Jacobs, A. Summers, B. Kolaczkowski, C. Goes, R. Fasano, Z. Mao, L. Al Homoud, K. Davis, and T. Overbye, "Harmonized automatic relay mitigation of nefarious intentional events (harmonie)-special protection scheme (sps)." Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2022.

[2] J. R. Aguero, E. Takayesu, D. Novosel, and R. Masiello, "Modernizing the grid: Challenges and opportunities for a sustainable future," *IEEE Power and Energy Magazine*, vol. 15, no. 3, pp. 74–83, 2017.

[3] A. Sahu, Z. Mao, P. Wlazlo, H. Huang, K. Davis, A. Goulart, and S. Zonouz, "Multi-source multi-domain data fusion for cyberattack detection in power systems," *IEEE Access*, vol. 9, pp. 119 118–119 138, 2021.

[4] L. Wei, A. I. Sarwat, W. Saad, and S. Biswas, "Stochastic games for power grid protection against coordinated cyber-physical attacks," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 684–694, 2016.

[5] J. Valenzuela, J. Wang, and N. Bissinger, "Real-time intrusion detection in power system operations," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 1052–1062, 2012.

[6] J. Qian, X. Du, B. Chen, B. Qu, K. Zeng, and J. Liu, "Cyber-physical integrated intrusion detection scheme in scada system of process manufacturing industry," *IEEE Access*, vol. 8, pp. 147 471–147 481, 2020.

[7] K. Martin, D. Hamai, M. Adamiak, S. Anderson, M. Begovic, G. Benmouyal, G. Brunello, J. Burger, J. Cai, B. Dickerson *et al.*, "Exploring the ieee standard c37. 118–2005 synchrophasors for power systems," *IEEE transactions on power delivery*, vol. 23, no. 4, pp. 1805–1811, 2008.

[8] A. Summers, C. Goes, D. Calzada, N. Jacobs, S. Hossain-McKenzie, and Z. Mao, "Towards cyber-physical special protection schemes: Design and development of a co-simulation testbed leveraging sceptre™," in *2022 IEEE Power and Energy Conference at Illinois (PECI)*. IEEE, 2022, pp. 1–7.

[9] L. Van der Maaten and G. Hinton, "Visualizing data using t-sne." *Journal of machine learning research*, vol. 9, no. 11, 2008.

[10] R. Gove, L. Cadalzo, N. Leiby, J. M. Singer, and A. Zaitzeff, "New guidance for using t-sne: Alternative defaults, hyperparameter selection automation, and comparative evaluation," *Visual Informatics*, vol. 6, no. 2, pp. 87–97, 2022.

[11] B. J. Kirby, J. Dyer, C. Martinez, R. A. Shoureshi, R. Guttromson, J. Dagle *et al.*, *Frequency control concerns in the North American electric power system*. United States. Department of Energy, 2003.

979-8-3503-1360-4/24/$31.00 ©2024 IEEE