Towards Real-Time Distinction of Power System Faults and Cyber Attacks on Digital Substations Using Cyber-Physical Event Correlation

Semertzis, Ioannis; Goyel, Himanshu; Rajkumar, Vetrivel S.; Presekal, Alfan; Stefanov, Alexandru; Palensky, Peter

DOI
10.1109/MSCPES62135.2024.10542753

Publication date
2024

Document Version
Final published version

Published in
Proceedings of the 2024 12th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)

Towards Real-Time Distinction of Power System Faults and Cyber Attacks on Digital Substations using Cyber-Physical Event Correlation

Ioannis Semertzis, Himanshu Goyel, Vetrivel S. Rajkumar, Alfan Presekal, Alexandru Ştefanov, Peter Palensky

Department of Electrical Sustainable Energy
Delft University of Technology
Delft, The Netherlands
I.Semertzis@tudelft.nl

2024 12th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES) | 979-8-3503-6284-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/MSCPES62135.2024.10542753

***Abstract* — Cyber actors can target the unsecured IEC 61850 protocols in digital substations to open circuit breakers and affect the power system operation. Thus, system operators must detect cyber-physical anomalies and differentiate in real-time between power system faults and cyber attacks on digital substations for effective incident response. In this work, we propose a novel image encoding method for event correlation using cyber-physical time-series data, i.e., Phasor Measurement Units (PMUs) and Operational Technology (OT) network traffic. More specifically, we propose a dynamic variation of the Gramian Angular Field method, which generates image streams capturing in real-time the spatial-temporal features in PMU measurements and IEC 61850 GOOSE traffic throughput. The proposed method for cyber-physical event correlation uses an image fusion technique. The method is tested using the benchmark IEEE 9-bus system. It successfully distinguishes between three-phase faults and GOOSE cyber attacks, demonstrating its usefulness for power system cyber security analytics.**

Keywords—Cyber attacks, cyber-physical power systems, cyber security, event correlation, IEC 61850, image encoding.

I. Introduction

Operational Technology (OT) communication networks are deployed for real-time monitoring and control of power grids. In the traditionally segregated OT domain, Information Technology (IT) solutions are being deployed to enhance the operational capabilities of the local control and monitoring systems. The lack of security measures like encryption and authentication makes the OT communication networks, e.g., IEC 61850, vulnerable to cyber attacks originating from the IT system. Cyber threat actors can target power system operations and conduct cyber-physical attacks. Cyber attacks on power grids are increasing and may lead to instability, loss of load, cascading failures, and a blackout [1], [2].

Considering the size and complexity of the power grid, the situational awareness of system operators needs to be enhanced to detect power system events, e.g., faults, in a timely manner and differentiate between physical events and cyber attacks. Under a faulted condition, protection relays detect and clear the short-circuit by opening the associated circuit breakers. However, the communication infrastructure inside the digital substation can be exploited to force a malicious trip or opening of circuit breakers, even in the absence of any electrical fault. System operators must identify the cause of the circuit breaker trip to mitigate the impact and maintain system stability based on limited information, i.e., power system measurements and alarms. Distinguishing these two situations is a challenging task due to the multi-domain nature of the problem, involving both physical and cyber elements. Intrusion Detection System (IDS) may be deployed in digital substations. However, stealthy cyber attacks may not be detected by IDS. Thus, the correlation between cyber and physical events, and eliminating the possibility of a power system fault are needed to improve the capability of cyber attack detection and mitigation.

Electrical power system fault detection and classification are well-studied fields, effectively captured by physical models or data-driven approaches using power system measurements [3]. However, a distinction between faults and cyber attacks on digital substations, both resulting in tripping circuit breakers, is non-trivial if only physical power system measurements are considered, e.g., Phasor Measurement Units (PMUs) and Supervisory Control and Data Acquisition (SCADA) measurements. This is due to the fact that the sequence of the cyber-physical events cannot be distinguished by examining measurements from a single layer, e.g., cyber or physical. In the case of faults, the physical operation change will precede the cyber one, as opposed to the case of cyber attacks. Additionally, detection of cyber attacks targeting power system operation needs to be performed in real-time, for effective incident response and mitigation. Related work in [4] and [5] utilized power system measurements from PMUs for distinguishing power system events and cyber attacks based on labels from IDS alerts. However, IDS alert datasets are required, which can be very challenging to generate. Furthermore, these methods require large labeled datasets of different attack scenarios. Thus, their deployment in power system control centers may be limited.

The availability of power system time-series data enables the application of data-driven methods for operational functions. In the context of this work, the recent advancements in image recognition algorithms led to the development of accurate methods for event classification problems. Thus, researchers are prompted to investigate methods for encoding power system time-series data to images. A promising method for encoding time-series measurements in 2D images is the Gramian Angular Field (GAF). In [6], PMU measurements were encoded using GAF and Short-Time Fourier Transform (STFT) for power system fault classification. In [7], the authors utilize GAF to encode measurement data that are used for multi-label classification of False Data Injection (FDI) attacks. In the aforementioned papers, the authors utilize the complete signals for GAF, and thus, this level of distinction

can be used in an offline manner and not in real-time. Additionally, in [7], the authors focus on the physical measurements obtained through the SCADA system, and they do not correlate them with communication network traffic for the detection of cyber attacks. Thus, the correlation between cyber-physical power system data for a real-time distinction of power system faults and cyber attacks is an open problem that is addressed in this paper.

In this work, we propose a novel image encoding method for event correlation using cyber-physical time-series data, i.e., PMUs and OT communication network traffic, to distinguish between three-phase faults and cyber attacks on digital substations. More specifically, we propose a dynamic variation of the GAF method, which generates image streams capturing in real-time the spatial-temporal features in PMU measurements and IEC 61850 Generic Object-Oriented Substation Event (GOOSE) traffic throughput. This method can be implemented in a power system control center, for increased situational awareness using cyber-physical event correlation and distinction. The scientific contributions of this paper are summarized as follows:

1) Formulating a novel data-driven method to encode in real-time cyber-physical time-series data into images.
2) Merging the continuous time and discrete event systems for cyber-physical system analysis.
3) Application of the proposed method for distinguishing between three-phase faults and IEC 61850 GOOSE spoofing attacks on digital substations.

II. Spoofing Attacks on Digital Substations and Distinction Challenges

In Fig. 1, the architecture of the digital substation using IEC 61850 standard is depicted along with the proposed application described in this paper. In this Section, the cyber attack investigated in this work is described, along with the necessary assumptions made to limit the research scope.

A. IEC 61850 GOOSE Spoofing Attacks

The IEC 61850 standard is utilized for communicating measurements and control signals in a digital substation. The standard specifies specific protocols, such as Sampled Values (SV) and GOOSE, which can be utilized for improved monitoring, protection, and control capabilities. Nevertheless, as these protocols were designed without cyber security considerations, e.g., lack of encryption and authentication mechanisms, they are vulnerable to cyber attacks. The focus of this work is mainly on spoofing attacks on the GOOSE protocol, which is used to communicate control commands between the protection Intelligent Electrical Devices (IEDs) and circuit breaker control IEDs, i.e., Bay Control Units (BCU).

The IEC 61850 standard specifies an object-oriented approach for defining the objects in a substation, and as such, the GOOSE protocol follows this approach. The hierarchy is defined as physical IED device, logical device, logical nodes, data objects, and data attributes [8]. A single IED can be used to represent multiple logical devices, which in turn can be used to represent multiple logical nodes. The payload of the GOOSE messages contains the breaker statuses and circuit breaker control commands. During normal operation, when there are no physical events, the protection IED issues GOOSE commands to the BCU periodically. The GOOSE messages are issued with a predefined time, ranging between 100 to 5,000 ms. In the case of a substation event, the messages associated with the event are issued at a higher rate of 0.5 to 4 ms. This is to achieve faster message exchange between the end devices within 3 - 4ms [9]. A GOOSE message has two important fields, “stNum” and “sqNum”. During normal operation, the “stNum” attribute remains constant while the “sqNum” increments with each new message being sent by the logical device. In the case of an event, the “stNum” attribute increments by one, and the “sqNum” is reset to zero [10]. Hence, to launch a successful GOOSE spoofing attack, the attacker manipulates these two fields along with the data attribute representing the circuit breaker status in the message. The attacker first performs snooping of the OT network traffic, capturing GOOSE packets flowing into the communication network. These captured frames are then modified by the attacker to have a high “stNum” such as 999, and zero “sqNum.” The attacker then injects these packets into the network. Since the manipulated message has a high stNum value, this supersedes the original message, which has a lower stNum value and causes the status of the circuit breaker to change [11]. Thus, by injecting spoofed GOOSE messages, cyber attackers can issue tripping commands that may open the circuit breakers, disconnect electrical circuits, disable interlocking, and block other substation equipment. Additionally, the “stNum” can be modified in such a manner that a consistency check will not discard the malicious packets [12].

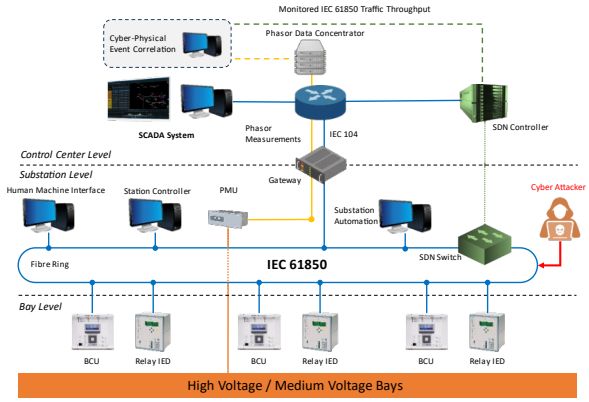


Fig. 1. Digital substation and control center architecture. The proposed method is applied centrally using PMU and IEC 61850 GOOSE traffic data.

B. Problem Statement

In case of a physical event such as a fault, the protection IEDs are expected to detect it and issue tripping commands to the BCU-connected circuit breakers. The timing mainly depends on the protection configuration and settings. For instance, for a three-phase fault that occurs in the middle of a transmission line connecting two substations, the distance relays detect and trip to open the circuit breakers in both substations, isolating the fault. As explained above, cyber actors may also issue malicious tripping commands directed to the BCUs, without the need for a physical event to occur. Additionally, it is important to mention that other breaker opening scenarios could be considered, such as malfunction of either the relays or circuit breakers, leading to an unwanted trip under normal conditions or not tripping / opening when a fault occurs. Finally, considering the capabilities of local and remote control from the system operators via the SCADA

system, opening commands could also be issued from the control center or substation control room to the BCUs without excluding the possibility of man-in-the-middle attacks. As such, the event classification problem can be quite complex. Amongst these possibilities, we are distinguishing between faults and cyber attacks on digital substations.

In this work, it is assumed that the cyber actors have compromised the substation network switch, which is used for message exchange between the process-level devices (BCUs) and the station-level devices (protection IEDs). Thus, the attackers are able to inject spoofed GOOSE messages, which can lead to malicious tripping of the BCU-connected circuit breaker. The aim is to utilize the combined cyber-physical data, which is obtained in the control center, to differentiate between a cyber attack scenario and power system faults.

C. Assumptions

Certain assumptions are made for the proposed method to be deployed in the control center. First, we assume that the integrity of the PMU data collected from the digital substations is assured. Second, we assume that PMUs are placed at all substations, meaning that all buses are monitored. Thus, the synchronized phasor measurements are transmitted from every substation to the control center, and they are available in a Phasor Data Concentrator (PDC). Furthermore, we assume that the GOOSE network traffic throughput from digital substations is available and monitored at the control center using Software-Defined Networking (SDN). SDN can be utilized to enable OT network traffic monitoring in substations, i.e., wide-area network monitoring, as in [13] and [14]. Using SDN, OT communication traffic throughput in the substations can be monitored from the control center. This is possible due to the segregation of SDN application into three layers, i.e., data plane, control plane, and management plane. In Fig. 1, the data plane is indicated with a blue line, and the control plane is indicated with a green line. The data plane is used for the main communication channel between substations and the control center. The SDN-enabled switch is able to monitor and report the OT communication network traffic throughput to the SDN controller (management plane) via the control plane. Finally, the power system is assumed to be $N-1$ secure, meaning that in the case of disconnection of a single element, it does not destabilize.

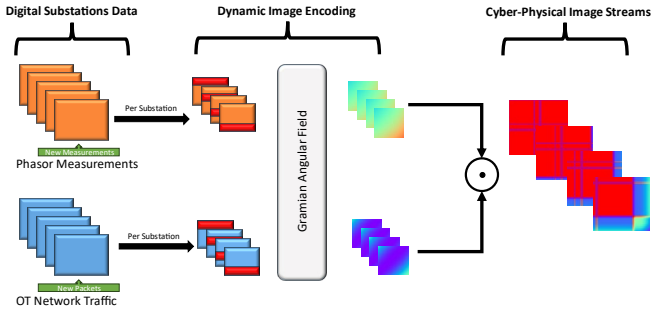


Fig. 2. Proposed dynamic image encoding method for cyber-physical data correlation.

III. Image Encoding Method for Event Correlation

In this study, the GAF algorithm is utilized for a real-time environment and is adapted for a continuous flow of data points. In the first part of this Section, the GAF algorithm is presented, while in the second part, the dynamic modifications made for the domain-specific task are presented. The proposed method is shown in Fig. 2.

A. GAF Algorithm

The GAF transformation was initially proposed in [15] as an algorithm to encode 1-D time series data into 2-D matrices. The novelty of the algorithm is its ability to retain at the same time the timestamp and amplitude information of the time series. Moreover, it can retain information hidden in the time series data and eliminate redundancy in the signal.

The time series data $X=\{x_1,x_2,...,x_n\}$ contains n real-valued numbers with the same time step, with n being the size of the time series. The first step of the GAF algorithm is to normalize the time series data between $[-1,1]$, utilizing the equation given in (1).

$$\tilde{x}_i=\frac{\left(\left(x_i-\max(X)\right)+\left(x_i-\min(X)\right)\right)}{\max(X)-\min(X)} \tag{1}$$

The rescaled values are normalized based on the maximum and minimum values of the specific time series data. The normalized time series data are then converted to the polar coordinate system. The conversion is achieved by taking the normalized elements as the cosine of the angle and by using the time step as the radius. This conversion is given in (2).

$$\tilde{X}(t)\rightarrow r\angle\phi:\begin{cases}\phi=\arccos(\tilde{x}_i), & -1\le\tilde{x}_i\le 1,\tilde{x}_i\in\tilde{x}_t\\ r=\dfrac{t_i}{N}, & t_i\in\mathbb{N}\end{cases} \tag{2}$$

where ϕ represents the angle in polar coordinates, r is the radius, t_i is the timestep, and N is a constant factor used to regularize the span of the polar coordinate. With the steps described above, the resulting transformed data have two important characteristics: 1) when the angle $\phi\in[0,\pi]$, it is bijective as the cosine function is monotonic and each time series produces a unique polar mapping image, and 2) the conversion of X to $\tilde{X}$ ensures that the angles are in the range of $[0,\pi]$.

Finally, the Gramian matrix is calculated using the cosine trigonometric sum between every two points of the angles data, which resulted from the transformation of the original data. The Gramian matrix is calculated as shown in (3).

$$\begin{aligned}G&=\begin{bmatrix}\cos(\phi_1+\phi_1) & \dots & \cos(\phi_1+\phi_n)\\ \vdots & \ddots & \vdots\\ \cos(\phi_n+\phi_1) & \dots & \cos(\phi_n+\phi_n)\end{bmatrix}\\ &=\tilde{X}'\cdot\tilde{X}-\sqrt{I-\tilde{X}^2}^{T}\sqrt{I-\tilde{X}^2}\end{aligned} \tag{3}$$

where I represents the unit row vector. The Gramian matrix defined above enables the usage of the angular perspective for the identification of the time relevance between each time interval. As a result, significant changes in the amplitude of the assessed signal can be captured, and the resulting image will show the transition in the bottom-right corner as the new data will be correlated with the past information. GAF contains the time correlation of the sequence because of the diagonal elements of the matrix.

B. Sliding Windows for Real-Time Encoding

In previous works, the GAF algorithm has not been utilized for real-time applications. The classification of the signal was performed utilizing static matrices, where multiple data points of the events were captured. As a result, the normalization procedure could be applied as in (1), as the major changes in the signal's magnitude were already present in the time series data. In this application, the GAF algorithm is utilized to construct a series of images that show the transition of the data as they are collected in real-time in the control center PDC and SCADA databases.

Sliding windows are utilized to modify the algorithm to be suitable for real-time applications. At every time step, the time series data X has a fixed length. As new measurements are collected in the control center, they are added to the time series dataset, and past measurements are extracted. An example is given as follows. The GAF algorithm is utilized to capture the PMU voltage magnitude transition for the past 3 s of operations and is updated every 1 s. Assuming that the PMU sampling rate in the control center provides 30 samples per s, for every new image, the 30 latest measurements are added to the time series data, while the oldest 30 measurements are omitted.

An additional issue arises due to the assessed minimum and maximum values of the dataset that are utilized for the initial normalization. If the normalization step is followed as specified in (1), the resulting image stream may have significant deviations. After a self-clearing three-phase fault occurs, and before the system stabilizes in a new equilibrium point, transient phenomena occur. If the sliding window size is small and the time series dataset contains only data regarding the oscillatory behavior, the resulting image will capture this behavior, regardless of the amplitude of the oscillation.

To address this issue, an algorithm is proposed for the maximum and minimum values that are used for the normalization of the time series data. In this algorithm, the past maximum and minimum values of the previous window are stored and used to capture the evolution of the signal. The algorithm is given in equations (4) to (6).

$$\tilde{x}_i = \frac{\left(\left(x_i - f\left(X_w, X_{w-1}\right)\right) + \left(x_i - g\left(X_w, X_{w-1}\right)\right)\right)}{f\left(X_w, X_{w-1}\right) - g\left(X_w, X_{w-1}\right)} \tag{4}$$

$$f\left(X_w, X_{w-1}\right) = \begin{cases} \max(X_w), & \max\left(X_w\right) > \max\left(X_{w-1}\right) \\ e^{\left(\frac{\max(X_{w-1}) - \max(X_w)}{\max(X_{w-1})}\right)} * \max\left(X_w\right), & otherwise \end{cases} \tag{5}$$

$$g\left(X_w, X_{w-1}\right) = \begin{cases} \min(X_w), & \min\left(X_w\right) < \min\left(X_{w-1}\right) \\ e^{\left(\frac{\min(X_w) - \min(X_{w-1})}{\min(X_w)}\right)} * \min\left(X_{w-1}\right), & otherwise \end{cases} \tag{6}$$

where $\max\left(X_w\right)$, $\min\left(X_w\right)$, $\max\left(X_{w-1}\right)$, and $\min\left(X_{w-1}\right)$ are the maximum and minimum non-negative values of the current and the previous time series window elements. In the case that the new data contains values that exceed the maximum and minimum thresholds, these values will be directly assessed in order for the normalization step to be correctly implemented. Otherwise, the new maximum and minimum values will be updated based on the difference between the old values and the new ones. As such, the new normalized values will be influenced by the previous state of the system, and the resulting series of images will have a smoother change.

C. Image Fusion for Cyber-Physical Event Correlation

The GAF method that is described above is used in both the cases of physical power system measurements and OT communication network traffic throughput to create images capturing the spatial-temporal correlation between their measurements. The advantage of the selected method is that the evolution of measurements in time is captured in the resulting images.

An important consideration for the proposed method is that the resulting GAF matrices should match not only in size but also in the timing that the measurements are collected. In this paper, a common time step is assumed for both the GOOSE communication network traffic throughput and PMU voltage magnitudes, e.g., 10 ms. This assumption is not always valid, and thus, fitting techniques should be applied, which are out of the scope of this work. The PMU voltage magnitudes and GOOSE network traffic throughput of each substation are continuously monitored. By covering a period of 1s, two GAF matrices are generated every 100 ms. As the matrices V_w, created using the PMU voltage magnitude measurements, and N_w, created using the GOOSE traffic throughput, have the same size, they can be used for a piecewise multiplication using the Hadamard product $\odot$. The main reason is that the position of each element of these two matrices captures the time information, which is extremely important for temporal correlation. The resulting matrix captures the combined cyber-physical information for the assessed time window.

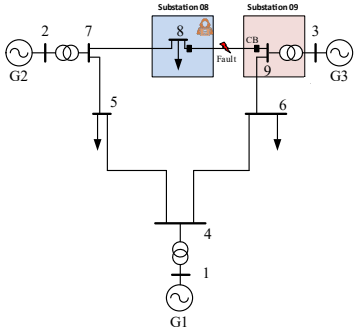
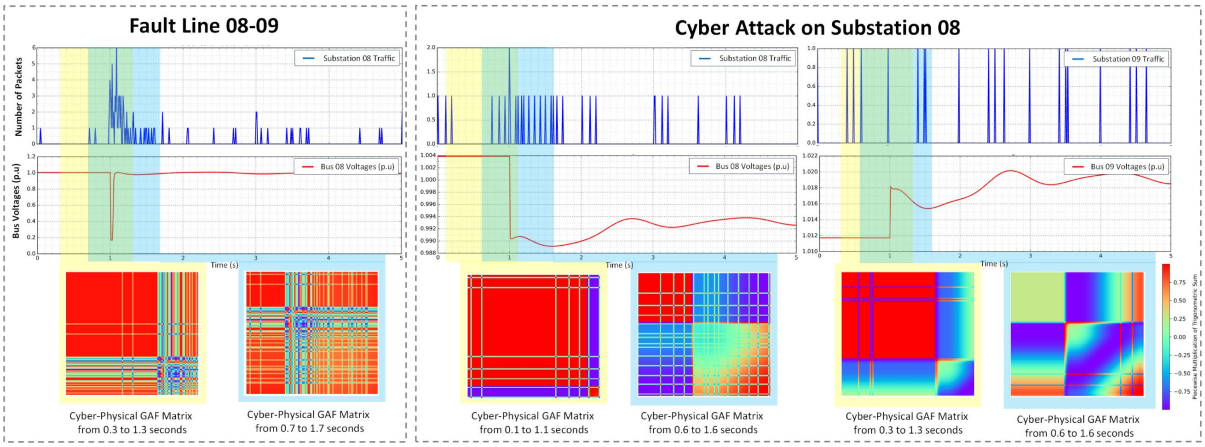


Fig. 3. IEEE 9-bus system with designated substations. Substation 08 is targeted by a cyber attack.

IV. Simulation Results and Discussion

A. Experimental Setup

The IEEE 9-bus dynamic model is implemented as the physical power system using the Real-Time Digital Simulator (RTDS). This transmission system model consists of synchronous generators, transmission lines, power transformers, and dynamic loads. The topology of the examined system is shown in Fig. 3. Time domain simulations are conducted to analyze the system dynamics and capture the physical response to a three-phase fault on line 08-09 and GOOSE spoofing attack targeting the substation 08. The results from the time domain simulations are exported capturing the PMU voltage magnitude measurements. The



(a) 3-phase fault, in the middle of line 08-09 (b) GOOSE spoofing attack on Substation 08 (c) Event correlation in Substation 09

Fig. 4. Cyber-physical event correlation using dynamic GAF images.

PMU measurements for each scenario are timestamped; thus, time series datasets are generated for each scenario. The loading of the power system is considered stable, and any change in its operating condition is the result of an event.

Regarding the OT communication network traffic present in a digital substation, we utilized a Hardware-in-the-Loop (HIL) testbed, using real protection IEDs that are connected through a network switch to the RTDS. The spoofed GOOSE messages are injected into the OT network traffic, as described in [16], while the capability of cyber attackers to compromise the substation network switch is out of scope of this work. To make the GOOSE traffic observed through a substation more realistic, multiple IEDs were connected in a digital substation OT network. The OT traffic throughput (in number of packets per 10 ms) is captured using Wireshark, where we filtered only the GOOSE packets. Finally, the proposed method and analysis are implemented using Python.

B. Cyber-Physical Operation of the Assessed Scenarios

For the physical power system, we monitor the RMS voltage magnitudes of each bus. We assume that each bus represents a substation, and PMUs are placed in each one. For the IEC 61850 network traffic, we capture the GOOSE packet throughput in one substation. This assumption is made for the monitored traffic per substation to represent an actual digital substation traffic, which means that the number of packets depends on the number of logical devices and logical nodes of each IED, as well as the number of IEDs that are present in the substation. The operation of the cyber-physical system per scenario is captured as follows:

1) In the case of a physical event, such as a short circuit, the physical measurements obtained with a high sampling rate from PMUs will capture significant changes in the operation of the power system. In the case of a three-phase fault, the voltage magnitude will drop significantly across the system as the power will flow through the low resistance to the ground. If the fault is permanent, it will be cleared by the actions of the protection devices. Considering the IEC 61850 GOOSE characteristics, the time of the protection tripping will be captured by the traffic throughput as a burst of packets. After the fault is cleared, the GOOSE traffic throughput will have a periodical behavior again.

2) In the case of the GOOSE spoofing attack, the cyber actors will craft malicious packets and inject them into the communication network traffic. For the BCUs to act on the spoofed commands, a continuous stream of packets is required to mimic the protection IED behavior. Achieving a burst of GOOSE packets that is exactly similar to the one issued by the protection IEDs in the digital substation is quite challenging. As a result, the GOOSE throughput will not be the same as that of the tripping of a protection relay. Furthermore, as the OT network traffic is altered before any physical event in the power system, the timing of the occurrence is extremely important for any distinction approach. Nevertheless, the circuit breaker will open, resulting in a physical change in the observed voltage measurements. This step change will be captured from all the installed PMUs.

C. Cyber-Physical Event Correlation using GAF

The proposed method for image encoding utilizing cyber-physical inputs is applied to the data collected using our HIL simulations. Two cases are assessed; one is a three-phase transmission line fault on line 08-09, while the second is the GOOSE spoofing attack on Substation 08, which results in the opening of the circuit breaker, connecting the same line to bus 08. The results are presented in Fig. 4.

For the first case, the three-phase fault is initiated at 50% of the line length between buses 08 and 09. The distance protection IEDs on both locations detect the fault, and they issue a burst of GOOSE packets, which leads to the opening of the circuit breakers on both locations and the disconnection of the affected line. The overall tripping and the breaker opening time is 0.038 s for both locations. In Fig. 4(a), this event is shown as captured on the side of bus 08. The fault occurs at 1 s simulation time. It is cleared at 1.038 s simulation time. Before the fault clearing, the voltage magnitude of the bus falls from 1.0 p.u. to 0.22 p.u. This step change is captured using the GAF method as the obtained measurement has a significant deviation compared to the measurements received up to 0.99 s. As a result, the correlation between the measurements, captured through the trigonometric sum of their transformed polar coordinates in the Gramian matrix, differs significantly. The same applies to the GOOSE network traffic throughput due to the burst of packets, which is encoded in the resulting image as square patterns. The reason is that the discrete communication network traffic is captured as a square signal. The fusion of the two images creates a

unique pattern, highlighting the fault's impact and duration, as well as the fact that voltage magnitude deviation occurred before the changes in the GOOSE network traffic throughput.

In the case of the GOOSE spoofing attack, and considering that the cyber attackers are not able to imitate the tripping response of the actual IED, the resulting image portrays malicious behavior in contrast to the previous case. Despite the steady operation of the power system, the substation's OT traffic throughput is increased due to the injection of the crafted packets in the communication network switch. Legitimate packets are also issued from the IEDs at the same time. After the breaker receives a stream of malicious packets, issuing a tripping command, it opens. The voltage magnitude measurements obtained after the event transpired significantly differ from the previous ones, as shown on the non-diagonal elements of the matrix. Furthermore, by merging the cyber and physical data into a common image, a distinction can be made based on the fact that initially the GOOSE traffic throughput changed, followed by the voltage magnitude. Additionally, an advantage of the dynamic GAF algorithm is highlighted: even though the voltage drop is 0.013 p.u., which is small compared to the previous case where it was 0.78 p.u., the event is captured sufficiently enough for the resulting dynamic GAF matrix to change. This is because the data of the dynamic time window are normalized based on the corresponding measurements. Thus, the method can detect small deviations in the cyber-physical time-series data which, when correlated, could be used for distinguishing an event.

Finally in Fig. 4(c), the same scenario is observed through Substation 09. To simulate this event, the digital substation configuration is assumed to be placed on Substation 09, while the cyber attack on Substation 08 was simulated in RTDS. In this case, as Substation 09 is not attacked, the GOOSE traffic throughput is unchanged and follows a periodic behavior, while the PMUs detect the event. Additionally, as the GAF matrix is generated through measurements obtained from a single substation, the evolution of the substation image captures the individual responses of these systems to an event.

Overall, the analysis presented above highlights the applicability of the proposed dynamic GAF method for encoding cyber-physical system data into a single image stream, retaining the spatial-temporal features of both. A fusion mechanism, e.g., piecewise multiplication of the cyber and physical GAF matrices, captures the unique cyber-physical system characteristics for event distinction. The proposed method merges the continuous time and discrete event systems. Analyzing the image stream of the correlated cyber-physical system data improves the operator capabilities to identify the cause of circuit breaker trips and detect cyber attacks. Finally, this method does not require a deep-packet inspection to provide meaningful results regarding the OT communication network traffic. Thus, it does not add significant latency to the overall processing time.

V. Conclusions and Future Work

In this paper, a novel image encoding method for event correlation using cyber-physical time-series data is proposed. By introducing a dynamic variation of the Gramian Angular Field method, the proposed algorithm is able to generate image streams in real-time, capturing the spatial-temporal features in power system measurements and OT communication network traffic throughput. The resulting images are fused, thus creating cyber-physical image streams, that are used for distinguishing between power system faults and cyber attacks on digital substations. The results show that by utilizing the proposed method, a clear distinction between faults and cyber attacks is possible. In future work, the proposed method will be evaluated for distinguishing additional cyber-physical events by considering additional signals. Additionally, a neural network model will be developed for image classification. More realistic operating conditions for the cyber-physical power system will be included to assess the performance of the proposed method, i.e., loading variations captured in the voltage measurements and communication network traffic jitter.

Acknowledgement

This work was supported by the RESCUE project funded by the Dutch Research Council (NWO ESI.2019.006).

References

[1] M. J. Assante et al., "ICS defense use case no. 6: modular ICS malware," *Electricity Information Sharing Center (E-ISAC) Tech. Report*, pp. 1-27, vol. 2, Aug. 2017.

[2] D. E. Whitehead et. al., "Ukraine cyber-induced power outage: analysis and practical mitigation strategies," in *Proc. Int. Conf. for Prot. Relay Engineers*, Texas, USA, Apr. 2017, pp. 1-8.

[3] X. Liang, S. A. Wallace, and D. Nguyen, "Rule-Based Data-Driven Analytics for Wide-Area Fault Detection Using Synchrophasor Data," *IEEE Trans. Ind. Appl.*, vol. 53, no. 3, pp. 1789-1798, May-June 2017.

[4] C. Hu, J. Yan, and C. Wang, "Robust Feature Extraction and Ensemble Classification Against Cyber-Physical Attacks in the Smart Grid," in *Proc. IEEE Elect. Power Energy Conf. (EPEC)*, Montreal, QC, Canada, 2019, pp. 1-6.

[5] G. Intriago, and Y. Zhang, "Online Dictionary Learning Based Fault and Cyber Attack Detection for Power Systems," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Washington, DC, USA, Jul. 2021, pp. 1-5.

[6] H. Ma, X. Lei, Z. Li, S. Yu, B. Liu, and X. Dong, "Deep-Learning Based Power System Events Detection Technology Using Spatio-Temporal and Frequency Information," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 13, no. 2, pp. 545-556, June 2023.

[7] M. Mohammadpourfard, I. Genc, S. Lakshminarayana, and C. Konstantinou, "Attack Detection and Localization in Smart Grid with Image-based Deep Learning," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Aachen, Germany, 2021, pp. 121-126.

[8] B. E. M. Camachi, O. Chenaru, L. Ichim, and D. Popescu, "A practical approach to IEC 61850 standard for automation, protection and control of substations," in *Proc. 9th Int. Conf. Electron., Comput. Artif. Intell. (ECAI),* Targoviste, Romania, 2017, pp. 1-6.

[9] D. Zheng, W. Zhang, S. N. Alemu, P. Wang, G. T. Bitew, D. Wei, and J. Yue, "Communication requirements of microgrids," in *Microgrid Protection and Control*, Academic Press, 2021, pp. 297-319.

[10] N. Kush, M. Branagan, E. Foo, and E. Ahmed, ''Poisoned GOOSE: Exploiting the GOOSE protocol,'' in *Proc. 25th Australas. Inf. Secur. Conf. (AISC)*, vol. 149, Jan. 2014, pp. 17–22.

[11] J. Parssinen, P. Raussi, S. Noponen, M. Opas, and J. Salonen, "The Digital Forensics of Cyber-Attacks at Electrical Power Grid Substation," in *2022 10th Int. Symp. Digital Forensics Secur. (ISDFS)*, Istanbul, Turkey, Jun. 2022, pp. 1-6.

[12] M. G. Silveira, and P. H. Franco, "IEC 61850 Network Cybersecurity: Mitigating GOOSE Message Vulnerabilities," in *Proc. 6th Annu. PAC. World Amer. Conf.*, USA, Aug. 2019, pp.1-9.

[13] M. Rezaee and M. H. Yaghmaee Moghaddam, "SDN-Based Quality of Service Networking for Wide Area Measurement System," in *IEEE Trans. Industr. Inform.*, vol. 16, no. 5, pp. 3018-3028, May 2020.

[14] A. Presekal, A. Ştefanov, V. S. Rajkumar and P. Palensky, "Attack Graph Model for Cyber-Physical Power Systems Using Hybrid Deep Learning," in *IEEE Trans. Smart Grid*, vol. 14, no. 5, pp. 4007-4020, Sep. 2023.

[15] Z. Wang, and T. Oates, "Encoding time series as images for visual inspection and classification using tiled convolutional neural networks," in *Proc. 29th Conf. Artif. Intell. Workshops (AAAI)*, 2015, pp. 1-7.

[16] V. S. Rajkumar, M. Tealane, A. Ştefanov, and P. Palensky, "Cyber Attacks on Protective Relays in Digital Substations and Impact Analysis," in Proc. *8th Workshop Model. Simulat. Cyber-Phys. Energy Syst*., Sydney, NSW, Australia, 2020, pp. 1-6.