IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 14 November 2024, accepted 2 December 2024, date of publication 11 December 2024,
date of current version 26 December 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3515642

RESEARCH ARTICLE

Tensor-Based Cybersecurity Analysis of Smart Grids Using IT/OT Convergence

DANIAL JAFARIGIV[1], (Member, IEEE), KEYHAN SHESHYEKANI[2], (Senior Member, IEEE), AND MARTHE KASSOUF[1], (Member, IEEE)

[1]Hydro-Québec Research Institute, Varennes, QC J3X 1S1, Canada
[2]Department of Electrical and Computer Engineering, Polytechnique Montreal, Montreal, QC H3T 1J4, Canada

Corresponding authors: Danial Jafarigiv (jafarigiv.danial2@hydroquebec.com) and Keyhan Sheshyekani (keyhan.sheshyekani@polymtl.ca)

This work was supported by the Mathematics of Information Technology and Complex Systems (MITACS) Accelerate Project in collaboration with Institute for Data Valorization (IVADO) and Hydro-Québec Research Institute.

ABSTRACT The expansion of cyberthreat landscape has been driving power utilities to investigate innovative methods for attack detection while leveraging the converged data generated across the grid Information Technology (IT) and Operational Technology (OT) systems. In this paper, we propose a tensor-based cybersecurity data analysis method and we prove its efficiency using tensors of IT and OT data obtained through the cosimulation of an electricity distribution system using wireless Long-Term Evolution (LTE) technology for synchrophasor communications. An approximate CANDECOMP/PARAFAC (CP) decomposition and Higher Order Singular Value Decomposition (HOSVD) are used to exploit the underlying hidden patterns in the low-rank data tensors. The effectiveness of the low-rank modeling using both decompositions is confirmed by demonstrating relatively low reconstruction error. A residual extraction method is also considered to distinguish the normal subspace of tensor dataset from the anomalous dataset resulting from the attacker actions. Finally, we highlight the intrusion detection performance of the proposed method compared to that of the Tensor Robust Principal Component Analysis (TRPCA) and the discrete-time nonlinear autoregressive neural network (NARX).

INDEX TERMS Cosimulation, CP decomposition, cyberattack, distribution grid, IT/OT convergence, LTE network, synchrophasor network, tensor decomposition.

I. INTRODUCTION

Distribution grids are evolving into smarter and more complex systems that can accommodate advanced metering and sensor technologies being developed for data gathering and grid intelligence [1]. In particular, fast and accurate measurements provided by synchrophasor technology and Advanced Metering Infrastructure (AMI) significantly improve monitoring and control of smart distribution grids [2]. However, with the proliferation of such systems that rely on high connectivity, smart distribution grids become increasingly exposed to malicious intrusions and cyberattacks. Prompt and effective detection of these events can be achieved through a comprehensive analysis of the data collected from the Phasor Measurement Units (PMUs), the smart meters and their supporting communications infrastructure. An appropriate testbed for grid operations and cybersecurity analyses can be obtained through the use of multi-scale and multi-physics simulators which are capable of integrating components and/or generating different synchrophasor network and distribution grid datasets [3]. The generated data consists of synchrophasor data as well as a large volume of multi-source and heterogeneous communication network data including Internet Protocol (IP) parsing packets, network traffic statistics, and flow tables. Tensor-algebraic formulations can be used to preserve and process multidimensional data in its original form. Accordingly, two types of dataset can be constructed namely communication network tensor and distribution grid tensor. The communication network tensor can be constructed using IP flow statistics

The associate editor coordinating the review of this manuscript and approving it for publication was Parul Garg.

(e.g., jitter, delay, ...) and time. Similarly, the distribution grid data can be represented as a tensor of bus variables (e.g., voltages, frequency, ...) and time [4].

Extending the application of traditional security solutions that are based on siloed IT security and OT security solutions is proving increasingly inefficient, thus, the need to develop new security solutions that leverage the large amount of multi-source input data, namely, the aggregation of the data generated by different communication network systems (IT) and by different control systems and electrical equipment (OT). This data can be used to simultaneously counteract different types of cyberattacks that can have various impacts on the distribution grid operations and the associated communication networks. For instance, the Denial of Service (DoS) attack gradually increases the traffic flow through flooding whereas the delay attack firstly causes a sharp increase in traffic flow and then reduces it [5]. Conversely, the impacts of False Data Injections (FDI) and replay attacks are more pronounced on the distribution system operation [6].

A. MOTIVATION

The growing exposure of power grids to cyberattacks has been motivating utility operators to enhance their cyberdefense capabilities including intrusion detection. The detection of cyberattacks targeting power systems is particularly challenging because of the increasing attack surface and sophistication on one hand, and because of the scarcity of data generated by real power systems under attack that can be used to build accurate intrusion detection algorithms, on the other hand. Traditional machine learning techniques are prone to several issues that make them unpractical for cybersecurity applications [5], [6]. The classical supervised learning approaches, such as signature-based techniques, are ineffective in operational contexts because it is impossible to characterize normal and abnormal behaviour upfront [7]. With the evolution of cyberattack tools and patterns, a cyberattack detection mechanism must address the unknown behaviour rather than detecting the known behaviour. Unsupervised approaches generally offer more efficient attack detection capability. However, these approaches rely on training a model using a large amount of data which can affect their training and testing time and limits their ability to deal with emerging patterns of sophisticated cyberattacks. Unsupervised techniques become more efficient if they are trained using the low-rank tensor extracted from the data rather than the data itself. Principle Component Analysis (PCA) is a widely used unsupervised technique for cyberattack detection that leverages the low-dimensional structure inherent in high-dimensional data [8]. Despite its wide application, PCA has a significant limitation in that it is sensitive to grossly corrupted or outlying observations, which are common in real-world data. Furthermore, PCA can only handle 2-way matrix data, which is a major drawback since real-world data is typically multidimensional.

Tensors are a natural way to express multidimensional data as an array of arbitrary dimensions which can discover complex correlations between multiple data attributes simultaneously [9]. The authors in [9] proposed a Tensor Robust Principal Component Analysis (TRPCA) to take advantage of tensor structure for the PCA technique. However, this technique can not capture the nonlinearities and extract the latent features. Conversely, tensor decompositions associated with unsupervised learning techniques factor data into components, each of which reflect a distinct pattern of the original data, and may be used to detect cyberattacks without the limitation of supervised techniques (learning incrementally) and linear unsupervised techniques such as TRPCA. In [10], the authors proposed a tensor decomposition technique to detect botnet activity in network traffic data. Tensor-based analysis approach for time series network measurements is used to detect anomalous patterns in the network traffic [11]. Also, some tensor-based techniques have been proposed for state estimation [12] and for the analysis of ambient oscillations [13] in power systems. One can use the tensor-based techniques to identify abnormal patterns in the power system measurements that may indicate a cyberattack. Tensor analysis is particularly effective when an attacker conceals an attack by impersonating regular behaviour and, thus, avoiding traditional detection techniques. If any pattern matched benign activity in all dimensions at the same time, it would not be identified as an attack (e.g., a natural equipment fault), else, there must be at least one dimension within which the attack can be recognized [14]. However, the choice of tensor-based technique will ultimately depend on the specific application and the characteristics of the data. The authors in [15] proposed a tensor completion technique to construct new stealthy FDI attack patterns by manipulating compromised measurements of IoT-based smart grid matching historical measurement patterns.

B. CONTRIBUTIONS

This paper proposes a tensor-based algorithm to carry out multidimensional data analysis while overcoming the aforementioned limitations of traditional machine learning techniques for cybersecurity applications in smart grids. In many analyses and classification approaches, low-rank tensor approximation plays an important role in dimensionality reduction, feature extraction and feature selection [16]. This paper, for the first time aims to extend the application of low-rank approximation of multiple tensors for cyberattack detection in smart distribution grids and its associated communication network. This study builds upon the thesis in [17], which aimed to develop a multi-agent Functional Mock-up Interface (FMI)-compatible cosimulation platform. This platform integrates simulators for power systems and communication networks to enhance cybersecurity analysis in smart grids by generating synthetic data. The main contributions of this paper are as follows:

1) Cosimulation of a Photovoltaic (PV)-based distribution grid and the associated communications network to

perform rigorous cybersecurity analysis: The cosimulation platform is not only used to simulate the attack and study its impact on the power grid, but also to generate the synthetic OT and IT data required to develop efficient intrusion detection techniques. To this end, a Long-Term Evolution (LTE) wireless communication-based synchrophasor network capable of tracing the packets and traffic flows is developed and simulated in NS-3. The distribution grid model including the PMUs are simulated in EMTP and the Phasor Data Concentrator (PDC) and the intrusion detection system are modeled and simulated in MATLAB/Simulink.

2) Evaluating the benefits of tensor-based intrusion detection data analysis by computing approximate CANDECOMP/PARAFAC (CP) decomposition and Higher Order Singular Value Decomposition (HOSVD) [18] and by using IT and OT data collected from the distribution grid and its associated communications infrastructure. To demonstrate the effectiveness of the proposed approach, a comparison with the linear TRPCA method is conducted.
3) Residuals extraction to perform anomaly detection and its comparison with the discrete-time nonlinear autoregressive neural network with exogenous inputs (NARX). This is important for the definition of new metrics for IT/OT convergence-based cyberattack detection.

The remainder of this paper is organized as follows: Section II provides a brief overview of tensor algebra and introduces the compression graph analysis and the residual extraction method. Section III proposes an offline multi-agent cosimulation platform and introduces a Long-Term Evolution (LTE)-based wireless synchrophasor network. In Section IV, the simulation results for the low-rank approximation and the outcomes of the cyberattack detection compared with other data analysis methods are presented. Concluding remarks are provided in Section V.

II. TENSOR ALGEBRA

The tensor notations and the tensor algebra terminologies used in this section are defined in the Appendix where the tensor decomposition and calculation methods are also presented.

A. LOW-RANK TENSOR SELECTION

We explore several ways to arrange IT and OT data in the form of tensors to obtain the optimal tensor decomposition in terms of the least reconstruction error. Then, to check whether there is a low-rank tensor structure in the IT and OT tensors, we use the compression graph (which depicts distortion vs. compression). The idea of using a compression graph coarsely resembles rate-distortion graph. We assess the performance of distortion (quality of the reconstructed data) by calculating the reconstruction error according to

$$e_{rec} = \frac{||\hat{\mathcal{T}} - \mathcal{T}||_{\mathrm{H}}^2}{||\mathcal{T}||_{\mathrm{H}}^2}, \tag{1}$$

where $\hat{\mathcal{T}}$ denotes the estimated tensor of the input tensor $\mathcal{T}$. Moreover, we assess the performance of the data compression by the Compression Ratio (CR), defined as the ratio of parameters in the low-rank model to the number of data samples in the original data. Consider $\mathcal{T} \in \mathbb{C}^{M_1 \times M_2 \times \ldots \times M_R}$ of rank R, then the number of parameters for $\mathcal{T}$ is:

$$M = \prod_{r=1}^{R} M_r \tag{2}$$

Accordingly, the numbers of parameters in the low-rank model of the CP decomposition and the truncated HOSVD of $\mathcal{T}$ are respectively given by [21]:

$$\text{CP (rank-d): } M_{CP} = \prod_{r=1}^{R} M_r \times d \tag{3}$$

$$\text{HOSVD (rank-d): } M_{HOSVD} = d^R + \prod_{r=1}^{R} M_r \times d \tag{4}$$

B. EXTRACTION OF RESIDUALS

In this section, we present a process to estimate the normal subspace model of a tensor and extract the residuals as the difference between the normal subspace model and the new input dataset. The normal subspace model can be obtained using tensor decomposition. The idea is to track the changes in the normal subspace and identify the anomalous subspace through residual analysis. In this paper, the proposed anomaly detection technique is based on the residuals derived from the CP decomposition. Tensor decomposition captures the normal subspace to construct the patterns, and anomalies are detected by evaluating deviations from the modeled patterns [11].

Let $\mathcal{T}_{(i,:,:)}$ be the i-th horizontal slice of tensor $\mathcal{T}$; a two-dimensional matrix obtained by fixing the first mode (first dimension of $\mathcal{T}$) at index i. Then, for each measurement of $\mathcal{T}_{(i,:,:)} \in \mathbb{C}^{1\times J\times K}$, we obtain an estimate model $\mathcal{V}_{(i,:,:)} \in \mathbb{C}^{1\times J\times K}$ using the CP decomposition and the ALS procedure [18]. In general, the residual $\mathcal{E}_{(i,:,:)} \in \mathbb{C}^{1\times J\times K}$ can be calculated as the difference between the input dataset and the model estimate $\mathcal{E}_{(i,:,:)} = \mathcal{T}_{(i,:,:)} - \mathcal{V}_{(i,:,:)}$. Having obtained the residual $\mathcal{E}_{(i,:,:)}$, we compute the residuals for new measurement datasets that were not previously used to parametrize estimated model $\mathcal{V}$. Let $\hat{\mathcal{T}}_{(k,:,:)}$ indicate the measurements corresponding to a new dataset for the first mode. The obtained factor matrices $\boldsymbol{B}$ and $\boldsymbol{C}$ from the previously estimated model $\mathcal{V}$ along with the new measurements $\hat{\mathcal{T}}_{(k,:,:)}$ can be used to construct vector $\hat{\boldsymbol{a}}(k) \in \mathbb{C}^{1\times R}$. Using the newly generated vector of $\hat{\boldsymbol{a}}(k) \in \mathbb{C}^{1\times R}$, the factor matrix $\hat{\boldsymbol{A}}_{(k,:)} = \hat{\boldsymbol{a}}(k)$ can be derived. Accordingly, the new model of $\hat{\mathcal{V}}_{(k,:,:)}$ with corresponding error of $\hat{\mathcal{E}}_{(k,:,:)}$ can be calculated using the factor matrices

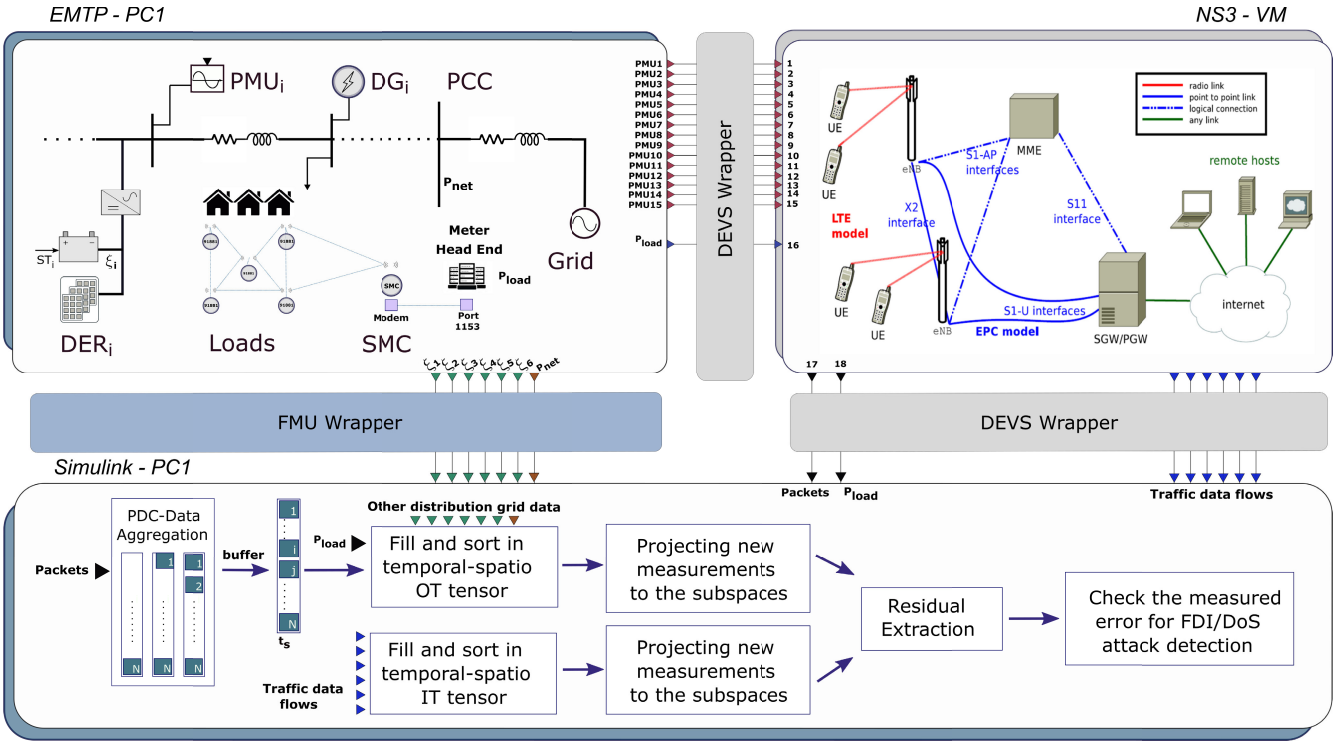


FIGURE 1. Cosimulation of the study system including: a) IEEE-123 bus test system in EMTP, b) LTE-based Synchrophasor network in NS-3, c) Tensor-based data processor in MATLAB/Simulink.

$\hat{\boldsymbol{A}}$, $\boldsymbol{B}$ and $\boldsymbol{C}$. Thus, the residuals of new dataset for the first mode are obtained by $\hat{\boldsymbol{\mathcal{E}}}_{(k,:,:)} = \hat{\boldsymbol{\mathcal{T}}}_{(k,:,:)} - \hat{\boldsymbol{\mathcal{V}}}_{(k,:,:)}$, where model $\hat{\boldsymbol{\mathcal{V}}}_{(k,:,:)} \in \mathbb{C}^{1\times J\times K}$ contains the new factor vector $\hat{\boldsymbol{a}}(k)$. The idea is to minimize quadratic error between model estimates $\hat{\boldsymbol{\mathcal{V}}}_{(k,:,:)}$ and measurements $\hat{\boldsymbol{\mathcal{T}}}_{(k,:,:)}$ using vector $\hat{\boldsymbol{a}}(k)$. Assume that $\hat{\boldsymbol{\mathcal{T}}}_{(k,:,:)(1)}$ is the matrix unfolding of tensor $\hat{\boldsymbol{\mathcal{T}}}_{(k,:,:)}$ in its first mode, where $\hat{\boldsymbol{\mathcal{T}}}_{(k,:,:)(1)} \in \mathbb{C}^{1\times JK}$. Then, we can write

$$\hat{\boldsymbol{\mathcal{E}}}_{(k,:,:)} = \hat{\boldsymbol{\mathcal{T}}}_{(k,:,:)} - \hat{\boldsymbol{\mathcal{V}}}_{(k,:,:)} \tag{5}$$

$$\hat{\boldsymbol{a}}(k)(\boldsymbol{C}\odot\boldsymbol{B})^{\mathrm{T}} = \hat{\boldsymbol{\mathcal{T}}}_{(k,:,:)(1)} \tag{6}$$

$$\hat{\boldsymbol{a}}(k) = \hat{\boldsymbol{\mathcal{T}}}_{(k,:,:)(1)}((\boldsymbol{C}\odot\boldsymbol{B})^{\mathrm{T}})^{\dagger} \tag{7}$$

Subsequently, we use the residual extraction of IT/OT tensor-based datasets to define new metrics for cyberattack detection.

In the following section, we describe an offline cosimulation platform that relies on the integration of multi-domain software tools to generate IT/OT tensor-based datasets and to derive spatio-temporal tensor-based correlations among the collected IT and OT data. This platform incorporates a distribution grid model and various power system components, including PMUs, to measure and transmit OT data via an LTE-based synchrophasor network model. The model simulates the communication network and includes data flow probes specifically designed for the collection of relevant IT data. The synthetic data generated by the co-simulation platform is then used to construct the IT and OT tensor structures. Finally, this platform is used to simulate a cyberattack scenario and to evaluate the effectiveness of the proposed tensor-based intrusion detection method.

III. COSIMULATION PLATFORM DESIGN

In this paper, we use offline cosimulation by integrating multi-domain software tools (namely MATLAB/Simulink, EMTP and NS-3) to model the operations of the distribution grid as depicted in Fig. 1. With access to real power grid data being difficult, this offline cosimulation platform can readily generate the required data for the operation modeling and the cybersecurity analysis of distribution grids and their supporting communication networks. Such data include the distribution bus data (i.e. synchrophasors, consumption and production power) and the statistics of the communication network traffic (i.e., throughput, delay, and jitter). These data will be used for offline tensor-based analysis. Furthermore, such cosimulation platform can be employed to derive the spatio-temporal tensor-based correlation among the collected IT and OT data. In our cosimulation platform, a Linux-based discrete-event simulator NS-3 interacts with the Windows-based Functional Mock-up Units (FMUs) generated from MATLAB/Simulink and EMTP. Integrating and interfacing these tools require dealing with different computing models, discrete and continuous variables, and various time-steps [22]. Compared to offline simulation, real-time simulation or Hardware-in-the-Loop (HIL) simulation has several limitations. The major constraint is the synchronization issue with external hardware, which

hampers the real-time simulation process. Additionally, the practical application of real-time simulation is limited to testing physical control and protection equipment, making it unsuitable for large-scale distribution grid simulation.

The NS-3 simulator operates on a significantly finer time resolution (nanosecond scale) than the FMUs which operate on a coarser timescale (millisecond scale). Therefore, a conversion process is necessary to align the timestamps of exchanged events between these two simulators. This transformation operation is incorporated into the coupling artifacts between NS-3 and the FMUs as can be seen in Fig. 2. The continuous equation-based models implemented in EMTP and MATLAB/Simulink are exported as FMU blocks and then integrated into the cosimulation platform as shown in Fig. 2. The EMTP solver runs its models and the imported FMUs from MATLAB/Simulink in asynchronous mode, in which both the host and client components perform their calculations independently at their respective time steps. The cosimulation core handles the data exchange between the FMUs (simulated in EMTP and MATLAB/Simulink) and the synchrophasor network, which is simulated in NS-3. Further details about the cosimulation platform performance can be found in [3].

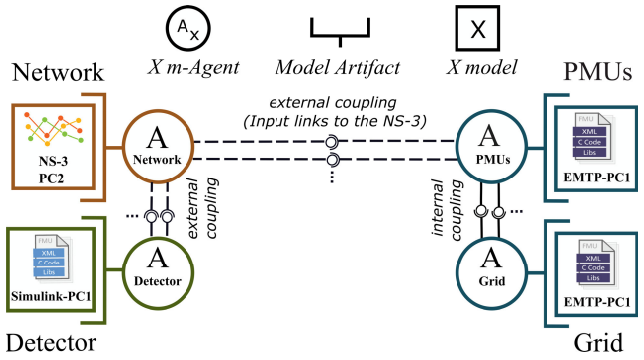


FIGURE 2. Cosimulation platform design including Models, Agents, Model artifacts, and Coupling artifacts.

The developed cosimulation platform exhibits great potential for conducting in-depth investigations into various aspects of distribution grid operations and cybersecurity. It is highly adaptable and can be easily leveraged to model and study the integration and the operations of different Distributed Energy Resources (DERs). Its flexibility and versatility make it well-suited for the simulation and impact analysis of different cyberattack scenarios as well as for the design and validation of appropriate mitigation strategies using advanced data analytic tools. Further details about the cosimulation platform performance can be found in [3].

A. DISTRIBUTION GRID MODEL

We use the IEEE-123 bus distribution system with a radial configuration as a test system to evaluate the performance of the proposed intrusion detection methods, as shown in Fig. 3. The test system operates at a nominal voltage of 24.9 kV and comprises 15 optimally placed PMUs to ensure complete observability. These PMUs are strategically assigned to substations with PV-based DER units, enabling each device to monitor a balanced portion of loads while capturing representative synchrophasor data across primary and secondary networks. Although practical distribution systems often deploy larger numbers of μPMUs for high-resolution measurements, our placement methodology revolves around achieving full observability with minimal redundancy and efficient data flow to the central distribution operation center [23]. Each load is equipped with a smart meter, and the data collected from these meters is gathered by a Smart Meter Collector (SMC). The collected data are transferred to the meter Head-End System (HES) and then to the substation central controller for voltage regulation purposes. The synchrophasor communication network that is used to transfer the PMU packets employs the LTE wireless communication technology as explained in the next subsection.

B. LTE-BASED SYNCHROPHASOR NETWORK MODEL

In this work, we consider an LTE-based wireless communication network interconnecting the PMUs of Fig. 3. The LTE is among the widely used cellular communication network standards for high-speed mobile devices that allow extensive installation and proliferation for Machine-to-Machine (M2M) communication [24]. Among the available communication technologies for synchrophasor networks, wireless communications can facilitate the transfer of synchrophasor data between geographically separated PMUs and Phasor Data Concentrators (PDCs). In some distribution grids, the large-scale wired-line based communication infrastructures are not flexible enough to easily support grid topology upgrades, which makes wireless communications the only feasible solution where Ethernet is not available. Owing to its low installation cost/time and flexibility, the LTE technology has recently attracted the attention of Distribution Network Operators (DNOs) for real-time synchrophasor data transmission [25]. However, this technology is characterized by relatively high delays, packet reordering, considerable data loss, and vulnerability to cyberattacks [26]. To properly address the availability and quality as well as the cybersecurity issues of synchrophasor data in the modern smart grids, communication latencies, impairments and cyberattack impact and remediation should be investigated. To facilitate these studies, one can resort to cosimulation platforms that model the LTE-based synchrophasor network. To the best of our knowledge, the LTE-based synchrophasor network has not been simulated yet using offline cosimulation platforms. In fact, the LTE communication for synchrophasor networks has only been studied through experimental validations [25]. In this paper, the performance and efficacy of the cybersecurity analysis method will be validated through elaborate cosimulation of LTE-based wireless synchrophasor network on a low-voltage distribution grid as shown in

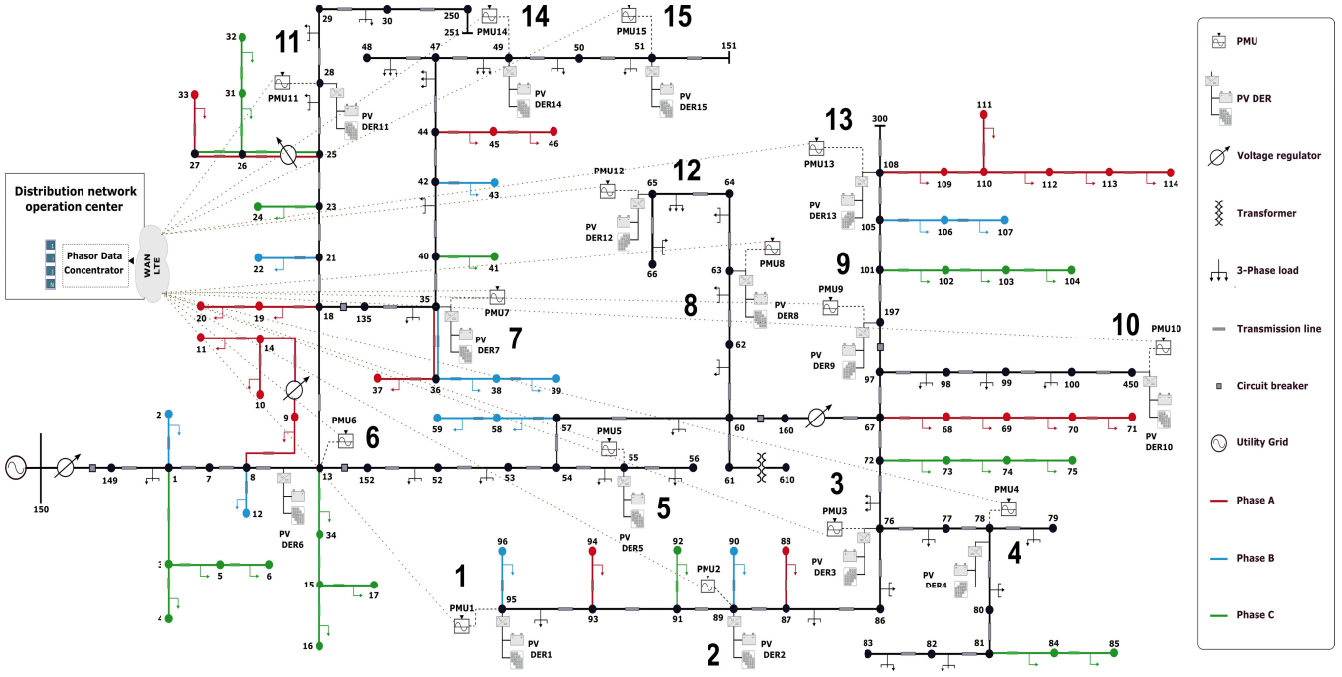


FIGURE 3. IEEE-123 bus distribution grid including PV systems and PMUs labeled with their substation number.

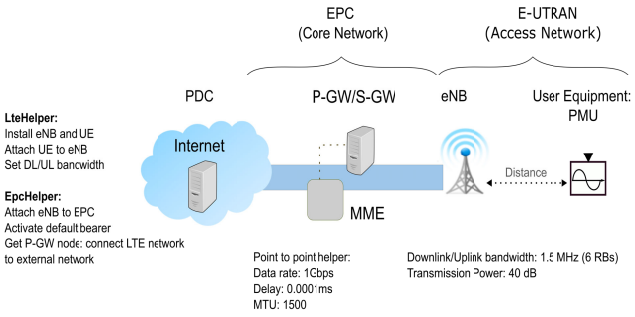


FIGURE 4. LTE implementation for a single UE and eNB.

Fig. 4. We chose to use User Datagram Protocol (UDP) for PMU data communications because it requires less overhead than Transmission Control Protocol (TCP)-based communications.

The LTE network has two main parts including Radio Access Network (E-UTRAN) and Enhanced Packet Core (EPC) [27]. To implement the LTE-based synchrophasor network in NS-3, we use the LTE/EPC module which consists of several network elements, including the User Equipments (UEs), LTE base station (eNodeB), EPC, and IP servers. The LTE/EPC module can be divided into two libraries. The main library (LteHelper) facilitates the evaluation of the following elements of LTE systems: 1) Radio Resource Management, 2) QoS-aware Packet Scheduling, and 3) Inter-cell Interference Coordination. The second library (EpcHelper) is used to model the EPC for supporting 1) the interconnection of multiple UEs to the internet, 2) IPv4-based Packet Data Network (PDN), and 3) S-GW (Serving Gateway) and P-GW (Packet Data Network Gateway) nodes implementation. To capture the LTE network data flow, we use the FlowMonitor module in NS-3 which contains one FlowMonitorHelper instance, one Ipv4FlowClassifier, and several Ipv4FlowProbes per Node [28]. Using this module, first, the probes collect packets before reporting to the global FlowMonitor abstract flow events, which are subsequently utilized for statistical data collection. Then the module requests the flow classifier to assign IDs to each packet. We use the following data flow attributes that are obtained through the FlowMonitor module in NS-3: 1) The **timeLastRxPacket** variable holds the absolute arrival time of the last packet in the flow, 2) The **timeFirstTxPacket** variable indicates the absolute departure time of the first packet in the flow, 3) **Duration** represents the difference between timeLastRxPacket and timeFirstTxPacket, 4) **txBytes** and **txPackets** reflect the total number of transmitted bytes and packets for the flow, respectively, 5) **rxBytes** and **rxPackets** indicate the total number of received bytes and packets for the flow, respectively, 6) **delaySum** is the sum of all end-to-end delays for the flow's received packets, 7) **jitterSum** is the sum of all end-to-end jitter (delay variation) values for the flow's received packets. Using these attributes, we can compute the metrics such as Mean Delay, Mean Jitter, and Throughput, presented in equations 8-10, which are essential for evaluating network performance and ensuring that quality of service (QoS) requirements are met:

$$\text{Mean Delay} = \frac{\text{delaySum}}{\text{rxPackets}} \tag{8}$$

$$\text{Mean Jitter} = \frac{\text{jitterSum}}{\text{rxPackets-1}} \tag{9}$$

$$\text{Throughput} = \frac{\text{rxBytes} \times 8}{\text{Duration}} \tag{10}$$

For the tensor-based data processor in MATLAB/Simulink, we collect and sort all the PMU packets using an advanced PDC structure shown in Fig. 1. An absolute waiting time is used to deal with the PMUs reporting latency and the communication network latency to push each time-tagged PDC dataset to the application, as described in [3]. The data are transmitted to the PDC through a dedicated gateway, which also serves as a firewall, ensuring safe connections for the DNO's center. The primary problems that DNOs confront in this context are cybersecurity and data streaming performance [26]. The PMUs transmit synchrophasor data at a rate of 60 frames per second (fps) to the PDC through dedicated LTE routers, using the communication protocol defined in the IEEE Std. C37.118.2 [29]. Each LTE router selects the closest LTE base stations (eNBs) among the three eNBs simulated in this network, as can be seen in Fig. 5. The downlink and uplink bandwidth is considered to have 6 resource blocks (1.4 MHz) with the transmission power of 40 dB for each base station. The UDP-based point-to-point communication link between the P-GW/S-GW and the remote host (PDC) has the data rate of 1 Gbps and the Maximum Transmission Unit (MTU) of 1500.

FIGURE 5. Multi-cell environment representation in NetAnim for the synchronized PMUs with the GPS signal.

C. IT AND OT TENSORS' STRUCTURES

We divide the data flows (IP flows) of the synchrophasor communication network into 15 channels to form a communication channel-oriented (or IT data) tensor. The associated three sets of variables collected for each channel are depicted on the right-hand side of Fig. 6: 1) jitter, 2) delay, and 3) throughput. Additionally, the distribution grid was divided into 15 substations based on electrical zoning and the geographical location of loads and generation sources, with

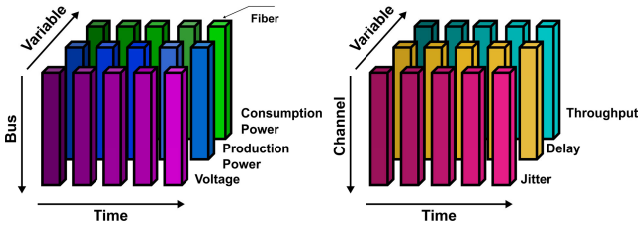


FIGURE 6. Bus-oriented (OT) and channel-oriented (IT) tensors (Mode-1 fibers).

each PMU monitoring a balanced portion of loads to avoid overloads on certain PMUs. Positioning the PMUs alongside the PV-ESS DERs substation allows for real-time monitoring of both power generation and consumption, enhancing the observability of distributed generation impacts on the grid. This approach depicts the entire distribution grid using 15 substations, each representing one PMU, one PV system, and several loads, to form a bus-oriented (or OT data) tensor. In this tensor structure, we investigate the correlation between variables. The associated three sets of variables collected from the distribution grid for each substation are depicted in the left hand side of Fig. 6: 1) voltage magnitude reported by the PMU, 2) consumption power of each substation reported by HES, and 3) production power based on the PV generation data.

D. A COMBINED FDI AND DOS CYBERATTACKS SCENARIO

In this paper, we focus on sophisticated cyberattacks for which the IT and OT data measured from the communication network and power system are subject to hardly detectable changes. Stealthy attacks with low detection probability would cause significant harm to the power grid systems. Considering a combined FDI and DoS attack scenario, we aim to find the most correlated tensor structure among the compromised measurements and develop a tensor-based attack detection algorithm using IT and OT data tensors. Tensor analysis may find complex correlations between multiple data variables at the same time since it operates in an arbitrary number of dimensions. This would allow for the identification of discrepancies between the data being received from the IT network and the expected values of the OT network. This can be particularly useful when the attacker conceals an attack by imitating normal behaviour, which renders intrusion detection very difficult using conventional data analytics.

For the FDI attack component of our scenario, it is assumed that the attacker injects false UDP frames through the synchrophasor network by manipulating the synchrophasors transmitted from the PMUs installed in the substations to the PDC, as shown in Fig. 3. We consider a case where the attacker targets the voltage values collected by the PMU2, PMU4, PMU5, PMU9 and PMU11 over the time interval [300, 700] min. This attack gradually increases the reported voltage values by 0.05 pu within 50 min, thus, impacting the whole distribution grid performance if not detected at the

right time. Moreover, we assume that the attacker launches the DoS component of the attack over the time interval [500, 600] min against the point-to-point communication link between the P-GW/S-GW and the PDC by knowing the IP address and port number of PDC. To this aim, the attacker is injecting legitimate UDP packets for 100 min with the rate of 150 Mbps using the attack pattern of timed square-wave packet burst. It is worth mentioning that low-rate DoS attacks unlike high-rate attacks are difficult to detect.

IV. SIMULATION RESULTS

We consider the distribution grid shown in Fig. 3. The experimental and large-scale fluctuations of solar irradiance data are taken from NRCAN [30] and used to simulate the time-varying power generation of PVs over a period of 16 hours. In this paper, the complete offline simulation time is 1000 min. The production power of PV based Distributed Energy Resources (DERs) is reported over the time interval of [300, 700] min for 15 substations in Fig. 7, which reveals the voltage fluctuation pattern induced by PV irradiance profiles. As can be seen in Fig. 8, the voltage profiles reported by 15 PMUs are within the permissible voltage deviation thresholds during normal operation.

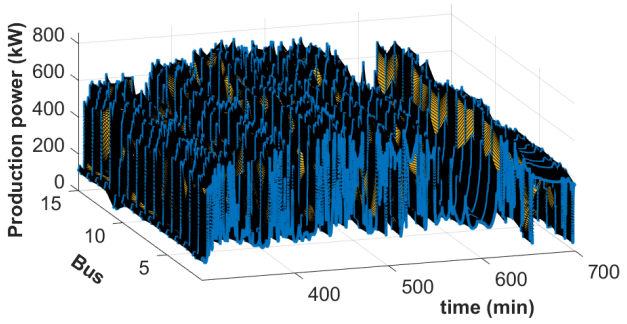


FIGURE 7. 3D representation of production power reported at each substation.

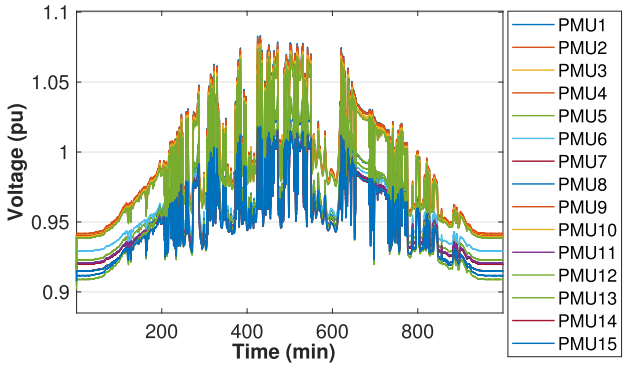


FIGURE 8. Voltage profiles reported by 15 PMUs.

Furthermore, the LTE communication network statistics of 15 flow data based on three attributes of jitter, delay, and throughput are collected. To have better insights into the delay distribution for the LTE network, Fig. 9 shows the relative frequency of each delay value for 15 IP flows. The IEEE C37.118.2 standard recommends a latency of less than 20 ms for the most restrictive PMU applications. As seen in Fig. 9, the delay values for LTE are more widely distributed, resulting in less deterministic transmission behaviour.

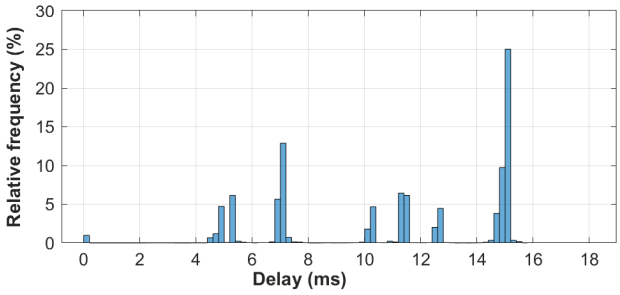


FIGURE 9. Uplink delay for LTE network at 15 channels, 120 fps.

We form the OT tensor and the IT tensor using the data generated by the cosimulation platform of Fig. 1 for the distribution grid and its associated communication network, respectively. These IT and OT data are arranged in the form of three-way tensors, as described in Section III-B and illustrated in Fig. 6. As a result, we manually selected $\mathcal{T}_{OT}$ for the distribution grid with orders of buses $\times$ time $\times$ variables and $\mathcal{T}_{IT}$ for the communication network with orders of channels $\times$ time $\times$ variables. We use Tensorlab 3.0 [31] and Tensortoolbox which are available in MATLAB for the tensor analysis. To apply the tensor decomposition effectively, the time interval of [300, 700] min is considered for both tensors as the most informative time window of the simulation. Therefore, the final dimensions of both tensors are $15 \times 40000 \times 3$. Also, each of the tensors has to be normalized, as the normalization of the tensors makes the distribution grid's and communication network's various amplitude scales and units consistent.

$$\mathcal{T}_{OT} = \frac{\mathcal{T}_{OT}}{||\mathcal{T}_{OT}||_{\mathrm{H}}} \quad \text{and} \quad \mathcal{T}_{IT} = \frac{\mathcal{T}_{IT}}{||\mathcal{T}_{IT}||_{\mathrm{H}}} \tag{11}$$

Next, we apply the tensor decomposition schemes of Section II to the generated tensors, resulting in various low-rank schemes. To evaluate the benefits of using tensor-based processing, we compute approximate CP and HOSVD decompositions. In fact, we consider two different algorithms ALS and SECSI (Appendix) to calculate the CP decomposition of three-way tensors. Typically, we gain from using tensors if the tensor has a low-rank structure that we can exploit. Therefore, there must be an underlying structure in the tensors of interest. We assess whether there is a low-rank tensor structure in the data by analyzing the compression graph of Fig. 10 that depicts the ratio of distortion versus compression. As seen from Fig. 10, rank-2 components indicate a significant fraction of the OT data in both HOSVD and CP decompositions.

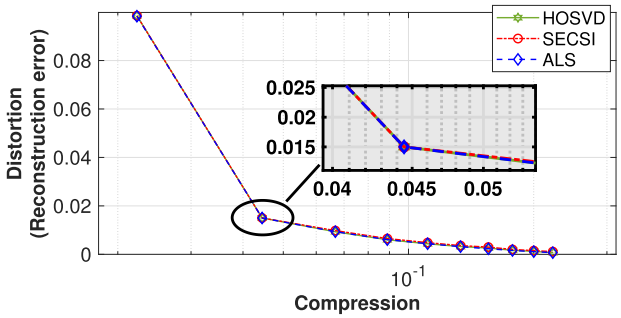


FIGURE 10. $\mathcal{T}_{OT}$ **Distortion (reconstruction error) vs. compression (number of parameters in the low rank model / number of data samples).**

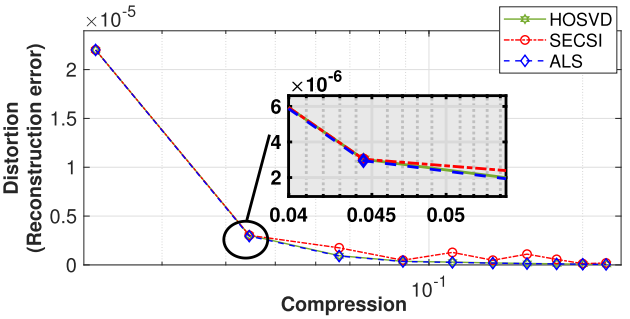


FIGURE 12. $\mathcal{T}_{IT}$ **Distortion (reconstruction error) vs. compression (number of parameters in the low rank model / number of data samples).**

The fraction of rank-2 components confirms that there is a low-rank structure. It is also interestingly seen from Fig. 10 that the reconstruction error for rank-2 component is about 0.015 when having only 4.4% of the samples. This enables cybersecurity professionals to compress the main tensor structure to rank-2 tensor without losing the correlated information that can be used for cyberattack detection. As can be seen in Fig. 11, a comparison between the reconstructed and original consumption power of substation 1 reveals the effectiveness of low-rank modeling. In terms of the type of variables, consumption power reconstruction has the smallest error of about 0.0371 for all methods in rank-2. It can be attributed to the fact that consumption power is a global quantity and the information from all locations contributes to data recovery. Voltage reconstruction shows a slightly larger error which is about 84.82, accounting for a 1.12% error.

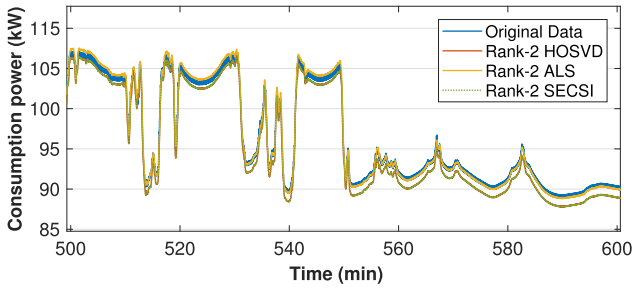


FIGURE 11. **Rank-2 reconstruction of original tensor for the consumption power at substation 1.**

Furthermore, as seen from Fig. 12, the rank-2 reconstructed component indicates a significant fraction in the IT data for both HOSVD and CP decompositions which proves that there is a low-rank structure. The reconstruction error for rank-2 component of both CP decompositions and HOSVD is about 3.032×10^{-6}. In fact, the components and their obtained reconstructed tensor exhibit a high quality for the compressed data in rank-2 which can be used to extract the multilinear subspace.

A. CYBERATTACK DETECTION

As explained in section III-D, the intruder launches the FDI component of the attack targeting the voltage values of PMU2, PMU4, PMU5, PMU9 and PMU11 over the time interval [300, 700] min. For the system under attack, the voltage reconstruction error for rank-2 reconstructed tensor is increased from 84.82 to 114.3670. Meanwhile, the reconstruction error for consumption and production power under attack remains constant, confirming that the attack must always be detectable in at least one dimension of the $\mathcal{T}_{OT}$. It is also observed that the reconstruction error is increased for the substations that encountered the attack, while remaining constant for the other substations. This approach can be used to distinguish an attack from equipment faults or other disruptive events that are not caused by malicious actions. Next, for the tensor $\mathcal{T}_{OT}$, we extract residuals of different cases, one with the FDI attack and the other one without the FDI attack, using the residual extraction techniques described in Section II-B. We divide our dataset into three distinct sets. The first set (T_{OT1}) contains the 15 solar irradiance profiles and is used to extract the normal subspace of tensor $\mathcal{T}_{OT}$. To fit the normal subspace using residuals derived from the tensor model, we utilize a second set (T_{OT2}) with a different solar irradiance profile. A third dataset (T_a) contains the FDI attack on voltage magnitude, which is utilized to demonstrate anomalous performance. The histogram presented in Fig.13 demonstrates that the selected datasets properly differentiate residuals of the cases with and without attack. This is due to the fact that the FDI attack footprint does not match the normal subspace in all dimensions of $\mathcal{T}_{OT}$ at the same time.

Regarding the DoS component of the attack scenario, we consider that the attacker launched DoS attack over the time interval [500, 600] min by targeting the point-to-point communication link between the P-GW/S-GW and the PDC. As shown in Fig 14, delay and jitter values for the IP flow of PMU1 are increased by 0.2 ms and 0.1 ms, respectively. These increases can be seen in all IP flows. During the attack, the delay reconstruction error for rank-2 reconstructed tensor $\mathcal{T}_{IT}$ is increased from 0.0002 to around 0.00055 and the jitter reconstruction error is increased from 5×10^{-4} to 9×10^{-4}. However, the reconstruction error for throughputs is not impacted by the DoS attack which again confirms that the attack is detectable in at least one dimension of the $\mathcal{T}_{IT}$.

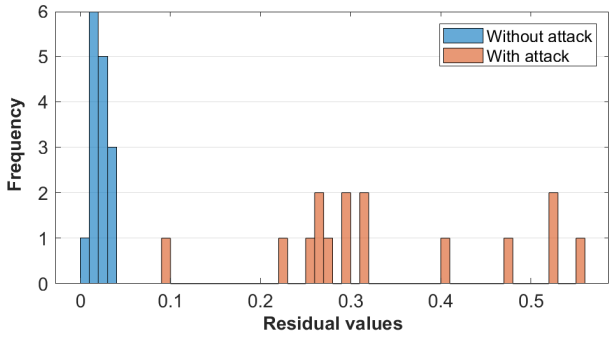


FIGURE 13. Histogram of residuals for two different cases of OT data.

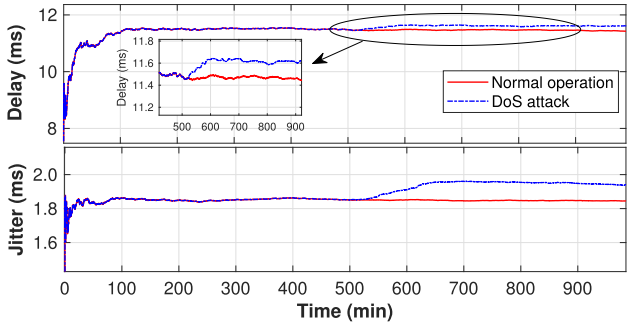


FIGURE 14. Impact of DoS attack on the IP flow of PMU1.

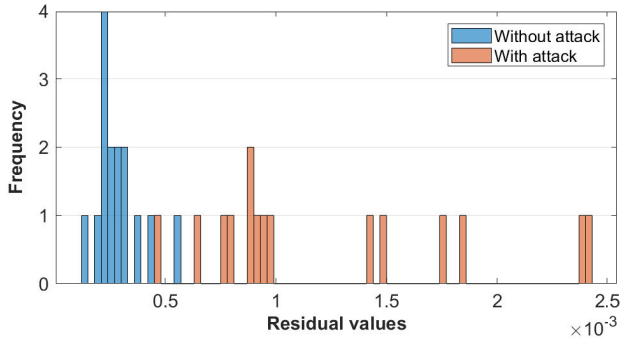


FIGURE 15. Histogram of residuals for two different cases of IT data.

Tensor residual extraction can be applied to the $\mathcal{T}_{IT}$ to detect the DoS attack by comparing the normal subspace obtained from the normal operation of synchrophasor network with the dataset of DoS attack. As can be seen in Fig. 15, the tensor residual extraction can differentiate the normal subspace from the DoS attack dataset.

In this paper, we considered IT and OT data tensors that have been analyzed in parallel which can be used to detect combined DoS attacks on the $\mathcal{T}_{IT}$ and FDI attacks on the $\mathcal{T}_{OT}$ or detect individual attacks. Further generalization of our method can be considered as a future work for the detection of combined complex attacks through the parallel processing of the IT and OT tensors. This would contribute to identifying the underlying attack zones and provide new insights for enhancing the distribution grid resilience against cyberattacks.

B. PERFORMANCE OF TENSOR DECOMPOSITION-BASED DETECTION METHOD

While tensor decomposition-based detection method has several advantages over other methods for cyberattack detection in power systems, it has the disadvantages of computational complexity and subjective interpretability. For high-dimensional data, the tensor decomposition can be computationally expensive and make it difficult for the real-time applications where fast detection and response to cyberattacks is required. In this work, the computation time to find the low-rank approximation and obtain the normal subspace of $\mathcal{T}_{IT}$ and $\mathcal{T}_{OT}$ with dimensions $15 \times 40000 \times 3$ was less than 3 minutes on a Windows-based machine with Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz processor and 16 GB RAM. Then every 3 minutes, the new tensors will be constructed using the new measured values, and the residuals will be extracted to detect the attacks. Using this approach, the computational time required for cyberattack detection will be relatively short while maintaining high efficiency, thus, allowing for near-real-time detection of cyberattacks. Such detection time can be further improved by using a more powerful machine with a higher processing speed. Moreover, the interpretable results depend on the order by which the IT and the OT data is arranged, which is determined by the test system structure. Therefore the approach proposed in section II-A should be followed to find the underlying structure in the tensors of interest for each test system.

C. COMPARISON WITH THE TRPCA AND NARX METHODS

In this section, we compare the performance of tensor decomposition method with a TRPCA approach for obtaining the low-rank tensor structure and exploring its efficacy in the context of cyberattack detection. The authors in [9] present a novel approach for tensor-based Robust Principal Component Analysis (RPCA) by introducing a tensor nuclear norm that captures the low-rank structure of tensors. This approach addresses the limitations of traditional RPCA methods, which are designed for matrix data and face challenges when applied to tensors. The TRPCA problem for tensor $\mathcal{M} \in \mathbb{C}^{I \times J \times K}$ can be presented as [9]:

$$\min_{\hat{\mathcal{L}},\hat{\mathcal{S}}} ||\hat{\mathcal{L}}||_* + \lambda||\hat{\mathcal{S}}||_1, \text{ s.t.} \quad \mathcal{M} = \hat{\mathcal{L}} + \hat{\mathcal{S}} \tag{12}$$

where the $\hat{\mathcal{L}}$ and $\hat{\mathcal{S}}$ represents the low rank component and the sparse component, respectively. The parameter λ is equal to $1/\sqrt{\max(I, J) \times K}$. This convex optimization problem can be solved using the standard Alternating Direction Method of Multiplier (ADMM) [9]. Further details about the nuclear norms and the ADMM can be found in [9]. By solving the TRPCA problem, we can recover the low-rank structure and spare components from their sum tensor $\mathcal{M}$. Using the TRPCA toolbox which is available in MATLAB [32],

we aim to get the low-rank model of the normalized $\mathcal{T}_{OT}$ and $\mathcal{T}_{IT}$ and compare the results with the tensor decomposition method described in Section II. To apply the TRPCA effectively, the time interval of [300, 700] min is considered for both tensors as the most informative time window of the simulation. The selected tolerance is $1e-5$ and the maximum number of iterations is 500. The step size for dual variable updating in ADMM is $1e-4$ and the λ for the normalized tensors of $\mathcal{T}_{OT}$ and $\mathcal{T}_{IT}$ is 0.00288. By applying the TRPCA on the $\mathcal{T}_{OT}$, we get the low-rank structure of a tensor with rank 3 which indicates the reconstruction error of 0.0222. However, for the system under attack, the reconstruction error of the measured tensor with rank 3 is decreased from 0.0222 to 0.0114. For the $\mathcal{T}_{IT}$, we also solved the same TRPCA problem to obtain the low-rank structure. The reconstruction error for $\mathcal{T}_{IT}$ is $1.592e-06$, while for the system under attack the reconstruction error of the measured $\mathcal{T}_{IT}$ is reduced to $9.35e-05$. These results indicate that the nonlinearities of the power system and the communication network measurements and their complex behaviour cannot be captured using the TRPCA method.

For further evaluation of the performance of the tensor-based attack detection approach, we compare the results of tensor-based residual extraction with the supervised learning approach proposed in [22]. To this aim, we develop neural network-based time-series algorithms for each of the IT and OT datasets to detect the attack scenario explained in III-D. The developed detection method is based on the discrete-time nonlinear autoregressive neural network with exogenous inputs (NARX), as discussed in [22]. In this case, the exogenous inputs are the consumption power and the production power for the OT dataset, while jitter and throughput are selected inputs for the IT dataset. As we can have only one target for NARX model, the target value for the prediction of a time-series using NARX for the OT and IT datasets are the voltage value measured by PMU4 and its IP flow delay, respectively. It is worth noting that the voltage profiles reported by PMUs shown in Fig. 8, with a good approximation, follow the same pattern of the PV total power fluctuations in Fig. 7. In other words, there is a nonlinear correlation between the voltage profiles and the PV total power fluctuations which can be an advantage for using the NARX method. While FDI attack impacts the measured voltage values of PMU4, it is interestingly seen that the predicted voltage values are not affected by the FDI attack. This is due to the fact that there is no change in the consumption power and the production power during the FDI attack. The difference between the predicted and the measured voltage values can be used for the detection of the FDI attack on the voltage values reported by PMUs. These results were validated and confirmed in our previous work [22].

However, the NARX model for the IT dataset can not track the fast dynamic behaviour of IP flow statics and predict the correct values of delay, as the throughput value is unchanged during the DoS attack and the jitter is affected by the DoS attack. This is due to the fact that there is a correlation between the delay and jitter and both are impacted by the DoS attack. It is worth mentioning that the developed NARX-based algorithm enables the detection of the FDI attack on the synchrophasor values, but is not able to detect the DoS attack on the IP flows' statistics. Moreover, one can note the complexity and the limitation of the NARX method for the prediction of multiple targets simultaneously. In fact, unlike tensor-based analysis, the NARX-based detection approach cannot operate on multiple targets, therefore, it is not able to look for the patterns in all dimensions at the same time.

In general, tensor-based analysis can handle multidimensional data naturally, capture nonlinearities of power system and communication network measurements, provide interpretable results to understand the underlying structure of the data, and apply to large datasets. Moreover, the tensor-based decomposition method provides robustness against missing or noisy data that can be encountered in power system measurements due to sensor failures or communication errors. By representing data as tensors, tensor algebra effectively captures complex correlations between multiple variables, allowing for better handling of missing and noisy data compared to traditional machine learning methods. These advantages render the tensor based decomposition method a promising solution over other unsupervised and supervised learning techniques for improving the cybersecurity of power systems. Furthermore, in order to implement a robust tensor-based intrusion detection system, it is important to address the existing barriers such as data integration, system complexity and computing resource constraints. This can be achieved by developing a comprehensive data integration plan that harmonizes and consolidates data from different sources. Implementing data normalization and mapping techniques ensures interoperability between disparate systems, while the use of data integration frameworks or middleware solutions facilitates smooth data exchange. Advocating for industry standards in data representation, communication protocols, and interoperability is essential, along with exploring cost-effective solutions such as cloud computing and outsourcing to overcome resource limitations.

V. CONCLUSION

This paper presented a tensor-based methodology for multidimensional IT/OT converged data analysis that overcomes the constraints of traditional machine learning techniques and contributes to the enhancement of distribution grid cybersecurity. By leveraging the strengths of tensor-based analysis, our approach effectively handles multidimensional data, captures nonlinearities in power system and communication network measurements, and provides interpretable results that clarify the underlying data structure. Using a co-simulation platform, we generated relevant IT and OT data to assess the efficiency of our method under a combined FDI and DoS cyberattack scenario targeting a PV-based distribution system with PMUs communicating over a wireless

Long-Term Evolution (LTE) network. To exploit the hidden patterns in the low-rank modeling of the collected IT/OT data, we computed approximate CANDECOMP/PARAFAC (CP) decomposition and Higher Order Singular Value Decomposition (HOSVD). Our simulations demonstrated the effectiveness of low-rank modeling, achieving a relatively low reconstruction error for just 4.4% of the samples (rank-2 components) across both decompositions. We compared these results with those obtained from the Tensor Robust Principal Component Analysis (TRPCA) method, which did not capture the impact of the cyberattack on the system. Additionally, our findings indicated that extracting the residual vector from tensor datasets can effectively identify all components of the cyberattack. Finally, we evaluated the performance of our tensor-based method against a neural network-based (NARX) time-series algorithm applied to the same datasets, revealing that the NARX method achieved only partial detection of the cyberattack components. In conclusion, while implementing a robust tensor-based intrusion detection system requires complex data integration methods and advanced computing resources, an enhancement in detection performance is observed, which would be crucial for grid operators to implement timely reponse to OT cyberattacks and to prevent potential service disruptions.

APPENDIX

In this paper the following notations are used: Scalars are signified by italic capital or lower-case letters, A, a. Vectors, matrices, and tensors are indicated by bold-faced lower-case letters $\boldsymbol{a}$, capital letters $\boldsymbol{A}$, and calligraphic letters $\boldsymbol{\mathcal{A}}$, respectively. Transposition, Hermitian transposition, matrix inversion, and Moore-Penrose pseudo matrix inversion are denoted by the superscripts $^{\mathrm{T}}$, $^{\mathrm{H}}$, $^{-1}$, and †, respectively [18]. The operators $||.||_{\mathrm{F}}$ and $||.||_{\mathrm{H}}$ represent the Frobenius and the higher order norms, respectively. The k-th 3-mode slice of $\boldsymbol{\mathcal{A}} \in \mathbb{C}^{I\times J\times K}$ is denoted as $\boldsymbol{\mathcal{A}}_{(:,:,k)}$ and one element is denoted as $\boldsymbol{\mathcal{A}}_{(i,j,k)}$. A superdiagonal or identity N-way tensor with dimensions $R \times R \ldots \times R$ is represented by symbol $\boldsymbol{\mathcal{I}}_{N,R}$. A tensor's inner product (scalar product) is defined as the sum of the product between all entries of the two tensors. Furthermore, an n-mode product of a tensor $\boldsymbol{\mathcal{A}} \in \mathbb{C}^{I_1\times I_2\times\ldots\times I_N}$ and a matrix $\boldsymbol{B} \in \mathbb{C}^{J\times I_n}$ is defined as $\boldsymbol{\mathcal{A}} \times_n \boldsymbol{B}$, for $n = 1, 2, \ldots N$.

$$\langle \boldsymbol{\mathcal{A}}, \boldsymbol{\mathcal{B}} \rangle = \sum_{ijk} \boldsymbol{\mathcal{A}}_{ijk}\boldsymbol{\mathcal{B}}_{ijk} = \langle \mathrm{vec}\,(\boldsymbol{\mathcal{A}}), \mathrm{vec}\,(\boldsymbol{\mathcal{B}}) \rangle \tag{13}$$

using Equation (13) we can define the higher order norm of a tensor and its relation with Frobenius norm as,

$$\begin{aligned} ||\boldsymbol{\mathcal{A}}||_{\mathrm{H}}^2 &= \langle \boldsymbol{\mathcal{A}}, \boldsymbol{\mathcal{A}} \rangle = ||\mathrm{vec}\,(\boldsymbol{\mathcal{A}})||_2^2 \\ &> = ||\boldsymbol{\mathcal{A}}_{(1)}||_{\mathrm{F}}^2 = ||\boldsymbol{\mathcal{A}}_{(2)}||_{\mathrm{F}}^2 = ||\boldsymbol{\mathcal{A}}_{(3)}||_{\mathrm{F}}^2 \end{aligned} \tag{14}$$

More fundamental tensor algebra terminology and definitions can be found in [18] and [19].

A. TENSOR DECOMPOSITIONS

The CP decomposition, or CANDECOMP (canonical decomposition) / PARAFAC (parallel factors) factorizes a tensor into a sum of the n-fold outer products of rank-1 tensors [18]. The CP tensor decomposition is an extension of the Singular Value Decomposition (SVD) to multidimensional arrays (tensors) [18]. Let $\boldsymbol{\mathcal{T}} \in \mathbb{C}^{I\times J\times K}$ of rank R, then a CP decomposition factorizes $\boldsymbol{\mathcal{T}}$ as a sum of rank one tensors, i.e.,

$$\begin{aligned} \boldsymbol{\mathcal{T}} &\simeq \sum_{r=1}^{R} \boldsymbol{a}_r \circ \boldsymbol{b}_r \circ \boldsymbol{c}_r = [\![\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}]\!] \\ &\simeq \boldsymbol{\mathcal{I}}_{3,R} \times_1 \boldsymbol{A} \times_2 \boldsymbol{B} \times_3 \boldsymbol{C}, \end{aligned} \tag{15}$$

where $[\![\ ]\!]$ denotes the CP decomposition operator and the operator "$\circ$" represents the vector outer product. The *rank* of tensor $\boldsymbol{\mathcal{T}}$ represents the lowest number of rank-one tensors that sum to $\boldsymbol{\mathcal{T}}$. The vectors $\boldsymbol{a}_r$, $\boldsymbol{b}_r$ and $\boldsymbol{c}_r$ are the corresponding columns of the factor matrices $\boldsymbol{A} \in \mathbb{C}^{I\times R}$, $\boldsymbol{B} \in \mathbb{C}^{J\times R}$ and $\boldsymbol{C} \in \mathbb{C}^{K\times R}$, respectively. The rank decompositions of higher-order tensors are "unique" which means that this is the only conceivable combination of rank-one tensors that sums to $\boldsymbol{\mathcal{T}}$. The HOSVD is another multilinear extension of the SVD and it is much easier to calculate than the CP decomposition. The HOSVD of the rank R tensor $\boldsymbol{\mathcal{T}} \in \mathbb{C}^{I\times J\times K}$ is given by [18],

$$\boldsymbol{\mathcal{T}} = \boldsymbol{\mathcal{S}} \times_1 \boldsymbol{U}_1 \times_2 \boldsymbol{U}_2 \times_3 \boldsymbol{U}_3, \tag{16}$$

where $\boldsymbol{\mathcal{S}} \in \mathbb{C}^{I\times J\times K}$ is the core tensor. The matrices $\boldsymbol{U}_1 \in \mathbb{C}^{I\times I}$, $\boldsymbol{U}_2 \in \mathbb{C}^{J\times J}$ and $\boldsymbol{U}_3 \in \mathbb{C}^{K\times K}$ are unitary matrices that span the column space of the n-mode unfolding of $\boldsymbol{\mathcal{T}}$, for $n = 1, 2, 3$, respectively. Accordingly, the truncated HOSVD $\boldsymbol{\mathcal{T}}^{[t]}$ is defined as

$$\boldsymbol{\mathcal{T}}^{[t]} = \boldsymbol{\mathcal{S}}^{[t]} \times_1 \boldsymbol{U}_1^{[t]} \times_2 \boldsymbol{U}_2^{[t]} \times_3 \boldsymbol{U}_3^{[t]}, \tag{17}$$

where $\boldsymbol{\mathcal{S}}^{[t]} \in \mathbb{C}^{R\times R\times R}$ is a truncated core tensor and the matrices $\boldsymbol{U}_1 \in \mathbb{C}^{I\times R}$, $\boldsymbol{U}_2 \in \mathbb{C}^{J\times R}$ and $\boldsymbol{U}_3 \in \mathbb{C}^{K\times R}$ have unitary columns.

B. COMPUTING THE CP DECOMPOSITION

Given $\boldsymbol{\mathcal{T}} \in \mathbb{C}^{I\times J\times K}$, and some target rank, R, finding the best R-rank approximation of $\boldsymbol{\mathcal{T}}$ is an NP-Hard problem:

$$\arg \min_{\hat{\boldsymbol{\mathcal{T}}}:\mathrm{Rank}_{CP}(\hat{\boldsymbol{\mathcal{T}}})\leq R} ||\boldsymbol{\mathcal{T}} - \hat{\boldsymbol{\mathcal{T}}}||_{\mathrm{F}} \tag{18}$$

A heuristic approach such as the Alternating Least Squares (ALS) algorithm 1 can be used to solve this NP-Hard problem [18].

Where $\odot$ holds for the Khatri–Rao product which is the column-wise Kronecker product. The ALS approach fixes $\boldsymbol{B}$ and $\boldsymbol{C}$ to solve for $\boldsymbol{A}$, and then fixes $\boldsymbol{A}$ and $\boldsymbol{C}$ to solve for $\boldsymbol{B}$, and then fixes $\boldsymbol{B}$ and $\boldsymbol{C}$ to solve for $\boldsymbol{A}$. Using Equation (18), this procedure is continued until a convergence condition is met. By fixing all matrices and solving the problem for one of them, the problem is simplified to a linear least squares problem:

$$\arg\min_{\hat{\boldsymbol{A}}} ||\boldsymbol{\mathcal{T}}_{(1)} - \hat{\boldsymbol{A}}(\boldsymbol{C} \odot \boldsymbol{B})^{\mathrm{T}}||_{\mathrm{F}} \tag{19}$$

Algorithm 1 Alternating Least Squares (ALS)

Require: Tensor $\mathcal{T}$ and target rank R

Ensure: $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$ each with R columns such that $\mathcal{T} \approx [\![\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}]\!]$

Ensure:

1: Initialize $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$ randomly
2: **repeat**
3: $\quad \hat{\boldsymbol{A}} \leftarrow \arg\min_{\hat{\boldsymbol{A}}} ||\boldsymbol{\mathcal{T}}_{(1)} - \hat{\boldsymbol{A}}(\boldsymbol{C} \odot \boldsymbol{B})^T||_{\mathrm{F}}$,
4: $\quad \hat{\boldsymbol{B}} \leftarrow \arg\min_{\hat{\boldsymbol{B}}} ||\boldsymbol{\mathcal{T}}_{(1)} - \hat{\boldsymbol{B}}(\boldsymbol{C} \odot \boldsymbol{A})^T||_{\mathrm{F}}$,
5: $\quad \hat{\boldsymbol{C}} \leftarrow \arg\min_{\hat{\boldsymbol{C}}} ||\boldsymbol{\mathcal{T}}_{(1)} - \hat{\boldsymbol{C}}(\boldsymbol{A} \odot \boldsymbol{B})^T||_{\mathrm{F}}$,
6: **until** < convergence >

the optimal solution of Equation (19) to find $\hat{\boldsymbol{A}}$ is given by [18]:

$$\hat{\boldsymbol{A}} = \boldsymbol{\mathcal{T}}_{(1)}(\underbrace{(\boldsymbol{C} \odot \boldsymbol{B})^{\mathrm{T}}}_{JK \times R})^{\dagger} \tag{20}$$

this is obtained directly from the fact that

$$\arg\min ||\boldsymbol{A}\boldsymbol{x} - \boldsymbol{b}|| = \boldsymbol{A}^{\dagger}\boldsymbol{b} \tag{21}$$

In our implementation of the ALS method, the convergence criterion for our algorithm is defined by a maximum limit of 3000 iterations, which prevents the algorithm from running indefinitely and ensures efficient use of computational resources. Additionally, we monitor the reconstruction error to assess convergence, setting a threshold of $\delta = 10^{-8}$. The algorithm will stop if the decrease in the reconstruction error is less than this threshold, indicating that further iterations are unlikely to yield significant improvements.

Another efficient semi-algebraic solution to compute the CP decomposition is to use simultaneous matrix diagonalization (SECSI) framework [20] that calculates all possible simultaneous matrix diagonalizations and then, in a final step, finds the best available solution using appropriate heuristics. In this paper, we utilize low-rank approximation methods via the CP and HOSVD decompositions to approximate OT and IT data. We consider two different algorithms of ALS and SECSI to calculate the CP decomposition of three-way tensors representing the IT and OT tensors.

REFERENCES

[1] M. Liu, "Enhancing cyber-resiliency of DER-based smart grid: A survey," *IEEE Trans. Smart Grid*, vol. 15, no. 5, pp. 4998–5030, Mar. 2024.

[2] B. Sun, Y. Xu, Q. Wang, S. Lu, R. Yu, W. Gu, and L. Mili, "Anomaly detection in data-driven coherency identification using cumulant tensor," *IEEE Trans. Power Syst.*, vol. 39, no. 2, pp. 4767–4770, Mar. 2024.

[3] D. Jafarigiv, K. Sheshyekani, H. Karimi, and J. Mahseredjian, "A scalable FMI-compatible cosimulation platform for synchrophasor network studies," *IEEE Trans. Ind. Informat.*, vol. 17, no. 1, pp. 270–279, Jan. 2021.

[4] B. Sandoval, E. Barocio, P. Korba, and F. R. S. Sevilla, "Three-way unsupervised data mining for power system applications based on tensor decomposition," *Electr. Power Syst. Res.*, vol. 187, Oct. 2020, Art. no. 106431.

[5] M. Khatua, S. H. Safavi, and N.-M. Cheung, "Sparse Laplacian component analysis for internet traffic anomalies detection," *IEEE Trans. Signal Inf. Process. Over Netw.*, vol. 4, no. 4, pp. 697–711, Dec. 2018.

[6] A. S. Musleh, M. Debouza, H. M. Khalid, and A. Al-Durra, "Detection of false data injection attacks in smart grids: A real-time principle component analysis," in *Proc. IECON 45th Annu. Conf. IEEE Ind. Electron. Soc.*, vol. 1, Oct. 2019, pp. 2958–2963.

[7] D. Bruns-Smith, M. M. Baskaran, J. Ezick, T. Henretty, and R. Lethin, "Cyber security through multidimensional data decompositions," in *Proc. Cybersecurity Symp. (CYBERSEC)*, Apr. 2016, pp. 59–67.

[8] A. Parizad and C. J. Hatziadoniu, "Cyber-attack detection using principal component analysis and noisy clustering algorithms: A collaborative machine learning-based framework," *IEEE Trans. Smart Grid*, vol. 13, no. 6, pp. 4848–4861, Nov. 2022.

[9] C. Lu, J. Feng, Y. Chen, W. Liu, Z. Lin, and S. Yan, "Tensor robust principal component analysis with a new tensor nuclear norm," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 42, no. 4, pp. 925–938, Apr. 2020.

[10] H. Kanehara, Y. Murakami, J. Shimamura, T. Takahashi, D. Inoue, and N. Murata, "Real-time botnet detection using nonnegative tucker decomposition," in *Proc. 34th ACM/SIGAPP Symp. Appl. Comput.*, Apr. 2019, pp. 1337–1344.

[11] A. Streit, G. Santos, R. Leão, E. de Souza e Silva, D. Menasché, and D. Towsley, "Network anomaly detection based on tensor decomposition," in *Proc. Medit. Commun. Comput. Netw. Conf. (MedComNet)*, Jun. 2020, pp. 1–8.

[12] R. Madbhavi, B. Natarajan, and B. Srinivasan, "Enhanced tensor completion based approaches for state estimation in distribution systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 9, pp. 5938–5947, Sep. 2021.

[13] J. J. Nuño-Ayón, E. S. Bañuelos-Cabral, J. Sotelo-Castañón, J. L. García-Sánchez, and J. A. Gutiérrez-Robles, "A tensor decomposition-based approach for the analysis and visualization of ambient power system oscillations," *Int. Trans. Electr. Energy Syst.*, vol. 31, no. 12, p. 13177, Oct. 2021.

[14] S. Rabanser, O. Shchur, and S. Günnemann, "Introduction to tensor decompositions and their applications in machine learning," 2017, *arXiv:1711.10781*.

[15] B. Liu, Y. Liu, and H. Wu, "Tensor-completion-enabled stealthy false data injection attacks on IoT-based smart grid," *IEEE Internet Things J.*, vol. 11, no. 22, pp. 36660–36672, Nov. 2024.

[16] A. G. Mahyari, D. M. Zoltowski, E. M. Bernat, and S. Aviyente, "A tensor decomposition-based approach for detecting dynamic network states from EEG," *IEEE Trans. Biomed. Eng.*, vol. 64, no. 1, pp. 225–237, Jan. 2017.

[17] D. Jafarigiv, "A scalable fmi-compatible cosimulation platform for smart grid cybersecurity studies using data analytics," Ph.D. dissertation, Dept. Elect. Comput. Eng., Polytechnique Montréal, Sep. 2021. [Online]. Available: https://publications.polymtl.ca/9238/

[18] T. G. Kolda and B. W. Bader, "Tensor decompositions and applications," *SIAM Rev.*, vol. 51, no. 3, pp. 455–500, Aug. 2009.

[19] A. Zare, A. Ozdemir, M. A. Iwen, and S. Aviyente, "Extension of PCA to higher order data structures: An introduction to tensors, tensor decompositions, and tensor PCA," *Proc. IEEE*, vol. 106, no. 8, pp. 1341–1358, Aug. 2018.

[20] F. Roemer and M. Haardt, "A semi-algebraic framework for approximate CP decompositions via simultaneous matrix diagonalizations (SECSI)," *Signal Process.*, vol. 93, no. 9, pp. 2722–2738, Sep. 2013.

[21] L. R. Tucker, "Some mathematical notes on three-mode factor analysis," *Psychometrika*, vol. 31, no. 3, pp. 279–311, Sep. 1966, doi: 10.1007/bf02289464.

[22] D. Jafarigiv, K. Sheshyekani, M. Kassouf, Y. Seyedi, H. Karimi, and J. Mahseredjian, "Countering FDI attacks on DERs coordinated control system using FMI-compatible cosimulation," *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1640–1650, Mar. 2021.

[23] Z. Zhao, H. Yu, P. Li, P. Li, X. Kong, J. Wu, and C. Wang, "Optimal placement of PMUs and communication links for distributed state estimation in distribution networks," *Appl. Energy*, vol. 256, Dec. 2019, Art. no. 113963.

[24] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

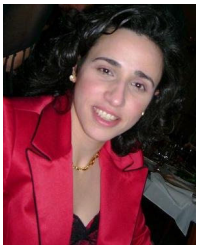
[25] A. Derviškadic, P. Romano, M. Pignati, and M. Paolone, "Architecture and experimental validation of a low-latency phasor data concentrator," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2885–2893, Jul. 2018.

[26] K. Pedramnia and M. Rahmani, "Survey of DoS attacks on LTE infrastructure used in AMI system and countermeasures," in *Proc. Smart Grid Conf. (SGC)*, Nov. 2018, pp. 1–6.

[27] M. Çakmak, "Performance comparison of queue management algorithms in LTE networks using NS-3 simulator," *Tehnički Vjesnik*, vol. 28, no. 1, pp. 135–142, 2021.
[28] G. Carneiro, P. Fortuna, and M. Ricardo, "FlowMonitor—A network monitoring framework for the network simulator 3 (NS-3)," in *Proc. 4th Int. ICST Conf. Perform. Eval. Methodologies Tools*, 2009, pp. 1–10.
[29] *IEEE Standard for Synchrophasor Measurements for Power Systems*, Standard C37.118.1-2011, 2011, pp. 1–61.
[30] NRCAN. *High Resolution Solar Radiation Datasets*. Accessed: Dec. 13, 2024. [Online]. Available: https://www.nrcan.gc.ca/energy/renewable-electricity/solarphotovoltaic/18409
[31] N. Vervliet, O. Debals, and L. De Lathauwer, "Tensorlab 3.0—Numerical optimization strategies for large-scale constrained and coupled matrix/tensor factorization," in *Proc. 50th Asilomar Conf. Signals, Syst. Comput.*, Nov. 2016, pp. 1733–1738.
[32] *Tensor Robust Principal Component Analysis (TRPCA) Based on a New Tensor Nuclear Norm*. Accessed: Dec. 13, 2024. [Online]. Available: https://github.com/canyilu/Tensor-Robust-Principal-Component-Analysis-TRPCA/tree/master

DANIAL JAFARIGIV (Member, IEEE) received the B.S. degree in electrical engineering from the Ferdowsi University of Mashhad, Iran, in 2012, the M.S. degree in electrical engineering from the Polytechnic University of Milan, Italy, in 2015, and the Ph.D. degree in electrical engineering from Polytechnique Montreal, Canada, in 2021. Since 2022, he has been a Cybersecurity Researcher with the Hydro Quebec Research Institute (IREQ), Varennes, QC, Canada. He has been contributing to various projects aimed at enhancing the cybersecurity of the power grid, primarily in the areas of modeling and co-simulation of cyber-physical systems, threat modeling, and cybersecurity risk analysis.

KEYHAN SHESHYEKANI (Senior Member, IEEE) received the B.S. degree in electrical engineering from Tehran University, Tehran, Iran, in 2001, and the M.S. and Ph.D. degrees in electrical engineering from the Amirkabir University of Technology (Tehran Polytechnique), Tehran, in 2003 and 2008, respectively. He was with the École Polytechnique, Fédérale de Lausanne, Lausanne, Switzerland, in September 2007, as a Visiting Scientist and later as a Research Assistant. He was an Assistant Professor and an Associate Professor with Shahid Beheshti University, Tehran, from 2010 to 2015 and from 2015 to 2016, respectively. He was an Invited Professor with EPFL, from June 2014 to September 2014. He joined the Department of Electrical Engineering, Polytechnique Montréal, Montréal, QC, Canada, in 2016, where he is currently a Full Professor. His current research interests include power system modeling and simulation, smart grids, and electromagnetic compatibility. He is an Associate Editor of IEEE TRANSACTIONS ON ELECTROMAGNETIC COMPATIBILITY.



MARTHE KASSOUF (Member, IEEE) received the B.Sc. degree in computer engineering from the École Supérieure des Ingénieurs de Beyrouth, Mansourieh, Lebanon, in 1997, the M.Sc. degree in computer engineering from the École Polytechnique de Montréal, Montreal, QC, Canada, in 1999, and the Ph.D. degree in electrical engineering from McGill University, Montreal, QC, Canada, in 2008. Since 2008, she has been a Researcher with the Hydro Quebec Research Institute (IREQ), Varennes, QC, Canada, where she has been contributing to the implementation of different projects aiming with the enhancement of the information and telecommunications infrastructure supporting the power grid, mainly in the areas of wireless communication systems, time synchronization, and cybersecurity. She has been the Project Manager for the cybersecurity research project with IREQ, since 2018. She is also an Adjunct Professor with the Department of Electrical and Computer Engineering, McGill University. Her research interests include telecommunication networks, time synchronization systems, power grid automation, and cybersecurity for smart grids. She has been a member in the Working Group 15 (WG15) of the International Electrotechnical Commission (IEC) Technical Committee (TC) 57, since 2015. She has been contributing to the development of IEC 62351 standards for the cybersecurity of power system information infrastructure.