

Cyberattack Detection in Large-Scale Smart Grids using Chebyshev Graph Convolutional Networks

Osman Boyaci

Electrical Engineering

Texas A&M University

College Station, TX, 77843

osman.boyaci@tamu.edu

M. Rasoul Narimani

College of Engineering

Arkansas State University

Jonesboro, AR, 72404

mnarimani@astate.edu

Katherine Davis

Electrical Engineering

Texas A&M University

College Station, TX, 77843

katedavis@tamu.edu

Erchin Serpedin

Electrical Engineering

Texas A&M University

College Station, TX, 77843

eserpedin@tamu.edu

Abstract—As a highly complex and integrated cyber-physical system, modern power grids are exposed to cyberattacks. False data injection attacks (FDIAs), specifically, represent a major class of cyber threats to smart grids by targeting the measurement data's integrity. Although various solutions have been proposed to detect those cyberattacks, the vast majority of the works have ignored the inherent graph structure of the power grid measurements and validated their detectors only for small test systems with less than a few hundred buses. To better exploit the spatial correlations of smart grid measurements, this paper proposes a deep learning model for cyberattack detection in large-scale AC power grids using Chebyshev Graph Convolutional Networks (CGCN). By reducing the complexity of spectral graph filters and making them localized, CGCN provides a fast and efficient convolution operation to model the graph structural smart grid data. We numerically verify that the proposed CGCN based detector surpasses the state-of-the-art model by 7.86% in detection rate and 9.67% in false alarm rate for a large-scale power grid with 2848 buses. It is notable that the proposed approach detects cyberattacks under 4 milliseconds for a 2848-bus system, which makes it a good candidate for real-time detection of cyberattacks in large systems.

I. INTRODUCTION

A modern power grid integrates the cyber communication network into the physical power system infrastructure. In this highly complex cyber-physical system, Remote Terminal Units (RTUs) deliver physical measurement data to the Supervisory Control and Data Acquisition Systems (SCADAs) [1]. Then, the communication network transfers these measurements to the application level in which they are processed by the Energy Management System (EMS). The security of the cyber-physical pipeline is critical as the secure and reliable operation of power grids strongly depends on the integrity of these data.

Integrity and validity of input data for the power system state estimation (PSSE) algorithm is crucial for the reliability of power grid operations as the output of the PSSE block is directly used by various EMS units such as forecasting of the load and analysis of contingency [2]. As one of the major classes of cyberattacks to the PSSE, false data injection attacks (FDIAs) aim to compromise the measurement data to bypass the bad data detection (BDD) algorithm and make the attack unobservable [3]. If the grid operator takes actions according to the false system state, s/he might jeopardize the security and reliability of the grid. Traditional BDD algorithms

for detecting FDIAs are insufficient as stealth (unobservable) cyberattacks can easily dodge these algorithms. Thus, FDIAs constitutes one of the most prominent threats to today's modern power grids.

FDIA detection algorithms are classified into two main categories as model-based methods and data-driven methods [4]. In model-based methods, a system model is built and its parameters are estimated. They do not require a historical dataset since they do not include any separate system to be trained. However, manual threshold optimization steps, high detection delays, and scalability issues limit their applicability for real time analysis. In contrast, data-driven methods eliminate the manual tuning steps, increase the scalability of the algorithm for attack detection, and reduce the detection time at the expense of a training process which need a historical dataset [4].

Recently, deep learning (DL) based data-driven detectors such as Fully-Connected Neural Networks (FCN) [5], Recurrent Neural Network (RNN) [6], Convolutional Neural Network (CNN) [7] have been proposed for cyberattack detection in power grids, thanks to the increasing volume of collected historical data samples. However, despite their powerful modeling capabilities, DL approaches may not generalize the data well enough and fail to detect cyberattacks if their architecture ignores the underlying physical system generating the data [4]. For instance, RNNs are perfectly suited architectures to model the recurrent structure of the language data. Similarly, CNNs are better candidates for image and video processing since sliding kernels are extremely efficient to exploit the pixel locality of image data [8].

Most of the works dealing with the detection of FDIAs ignore the spatial correlation of the power grid data, therefore, they fail to fully model the underlying graph topology of the power grid. There is only a few works [9], [10] in the literature that exploit the spatial correlations of the power grids to detect cyberattacks using Graph Signal Processing (GSP). Although GSP offers highly efficient tools for cyberattack detection, the custom design steps of spectral filters and scalability problems restrict its usability in real life scenarios. As a data-driven version of GSP, Graph Convolutional Networks (GCN) predict the filter weights in their hidden layers and eliminate the manual filter design steps. This automation makes GCNs more

attractive to power grid applications, for instance, GCNs are utilized for optimal power flow applications of power grids in [11], for cyberattack detection in [12], and for cyberattack localization in [13].

Scalability and detection time are the most fundamental factors in designing cyberattack detectors as the number of units varies between tens to a few thousand in today's power grids. Except a few highly scalable models including [12]–[15], most of the proposed models for cyberattack detection are designed for small-scale systems such as IEEE 14- [16]–[19] and IEEE 30- [6], [20] bus test systems. Scalability problems may appear as high detection delays when small-scale models are applied to large-scale networks.

In this work, we propose a cyberattack detection model that utilizes Chebyshev Graph Convolutional Networks in its hidden layers, enabling it to fully exploit the spatial correlations of the smart grid data. We integrate the grid topology to our detector with the weighted graph adjacency matrix obtained by grid's admittance matrix represented with \mathbf{Y}_{bus} . To train the proposed model, we generate a historical dataset having 36000 samples for a large-scale smart grid with 2848 buses. We verify the proposed detector by implementing two of the frequently used cyberattack models and comparing the detection results with the existing architectures designed for cyberattack detection.

The contributions of this work are summarized as follows:

- We design a deep learning architecture by employing Chebyshev Graph Convolutional Networks in its hidden layers to adequately capture the spatial correlations of graph structural smart grid data.
- We propose a model to detect cyberattacks in a few milliseconds even for large-scale grids with more than 2000 buses.
- The proposed model has an end-to-end automatic training process without having any custom optimization step.

The rest of this paper is organized as follows. While Section II formulates the problem, Section III proposes the FIDA detection method using GCNN. Results and discussion are presented in Section IV. Section V concludes the paper.

II. PROBLEM FORMULATION

In power grids, system state $\mathbf{x} \in \mathbb{R}^n$ is calculated in PSSE block using complex measurements $\mathbf{z} \in \mathbb{R}^m$ as follows:

$$\hat{\mathbf{x}} = \arg \min_{\mathbf{x}} \|\mathbf{z} - h(\mathbf{x})\|^2. \quad (1)$$

where \mathbf{x} represents bus voltage magnitudes/angles (V_i, θ_i), and \mathbf{z} denotes the active/reactive power injections at buses (P_i, Q_i), $h(\mathbf{x})$ is the nonlinear equations vector correspondent to the flows on branches (P_{ij}, Q_{ij}) that can be represented by

AC power flow equations in (2):

$$\begin{aligned} P_i &= \sum_{j \in \Omega_i} V_i V_j (G_{ij} \cos \theta_{ij} + B_{ij} \sin \theta_{ij}) = P_{Gi} - P_{Li} \\ Q_i &= \sum_{j \in \Omega_i} V_i V_j (G_{ij} \sin \theta_{ij} - B_{ij} \cos \theta_{ij}) = Q_{Gi} - Q_{Li} \\ P_{ij} &= V_i^2 (g_{si} + g_{ij}) - V_i V_j (g_{ij} \cos \theta_{ij} + b_{ij} \sin \theta_{ij}) \\ Q_{ij} &= -V_i^2 (b_{si} + b_{ij}) - V_i V_j (g_{ij} \sin \theta_{ij} - b_{ij} \cos \theta_{ij}). \end{aligned} \quad (2)$$

where Ω_i represents the set of buses connected to bus i ; $G_{ij} + jB_{ij}$ corresponds to the ij^{th} elements of bus admittance matrix \mathbf{Y} ; and $g_{ij} + jb_{ij}$ denotes the series branch admittance between buses i and j , respectively.

PSSE unit can be vulnerable to cyberattacks because if an adversary has 'enough' knowledge about the power grid, s/he can shift the system state from its original value by injecting some false data to the measurements. In other words, if the adversary find vectors $\mathbf{a} \in \mathbb{R}^m$ and $\mathbf{c} \in \mathbb{R}^n$ that satisfy equation (3), then they can easily add their attack vector \mathbf{a} to the \mathbf{z} and shift the state vector by \mathbf{c} from its original value \mathbf{x} without being detected by traditional BDD algorithms.

$$\mathbf{z} + \mathbf{a} = h(\mathbf{x} + \mathbf{c}), \quad (3)$$

III. CYBERATTACK DETECTION BY CHEBYHSEV GRAPH CONVOLUTIONAL NETWORKS

A. Chebyshev Graph Convolution

Power system variables such as \mathbf{P} , \mathbf{Q} , \mathbf{V} , and $\boldsymbol{\theta} \in \mathbb{R}^n$ can be represented as graph signals by modeling the power grid as a graph. Specifically, if we map buses to vertices \mathcal{V} ($|\mathcal{V}| = n$), branches and transformers to edges (\mathcal{E}), and line admittances to weighted adjacency matrix ($\mathbf{W} \in \mathbb{R}^{n \times n}$), we can efficiently represent the power grid topology with a connected, undirected, weighted graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathbf{W})$. For \mathcal{G} , the normalized graph Laplacian can be given by (4).

$$\mathbf{L} = \mathbf{I}_n - \mathbf{D}^{-1/2} \mathbf{W} \mathbf{D}^{-1/2} \in \mathbb{R}^{n \times n} \quad (4)$$

The Laplacian, i.e. \mathbf{L} is an essential operator in the theory of GSP. Since \mathbf{L} is a real, symmetric, and positive semi-definite matrix, it can be factorized as $\mathbf{L} = \mathbf{U} \boldsymbol{\Lambda} \mathbf{U}^T$ where $\mathbf{U} = [\mathbf{u}_0, \dots, \mathbf{u}_{n-1}] \in \mathbb{R}^{n \times n}$ denotes the n orthonormal eigenvectors, and $\boldsymbol{\Lambda} = \text{diag}([\lambda_0, \dots, \lambda_{n-1}]) \in \mathbb{R}^{n \times n}$ corresponds n eigenvalues of \mathcal{G} . Indeed, \mathbf{u}_i and λ_i values form the Fourier basis and Fourier frequencies in spectral domain of \mathcal{G} [21].

Different from classical signal processing, there is no meaningful translation operation in the vertex domain [22]. Thus, to filter a vertex domain graph signal $\mathbf{x} \in \mathbb{R}^n$ with a filter g_θ defined on \mathcal{G} , \mathbf{x} is first transformed into the spectral domain using Graph Fourier Transformation (GFT) by $\tilde{\mathbf{x}} = \mathbf{U}^T \mathbf{x}$. Next, the spectral domain signal $\tilde{\mathbf{x}} \in \mathbb{R}^n$ is filtered in the spectral domain by $\tilde{\mathbf{y}} = g_\theta(\boldsymbol{\Lambda}) \tilde{\mathbf{x}}$ where $g_\theta(\boldsymbol{\Lambda}) = \text{diag}(\theta)$ is a filter kernel, and $\boldsymbol{\theta} \in \mathbb{R}^n$ is a vector of Fourier coefficients [21]. Finally, the result is transformed back to the vertex domain using inverse GFT by $\mathbf{y} = \mathbf{U}^T \tilde{\mathbf{y}}$ [22].

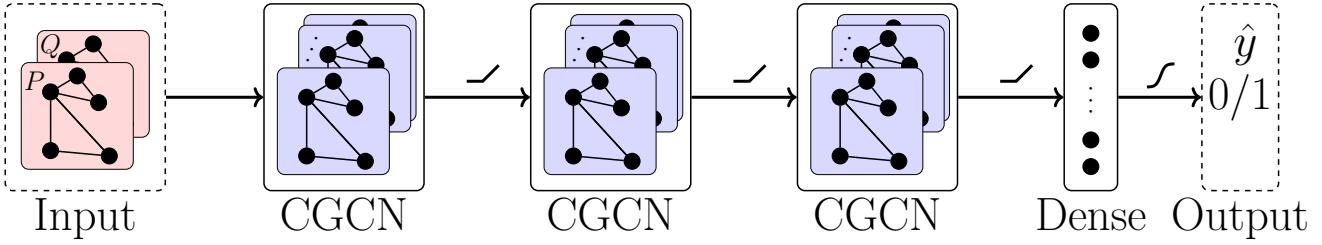


Fig. 1. Architecture of the proposed GNN based detector. It takes active and reactive bus power injections \mathbf{P} and \mathbf{Q} as its inputs, extracts their spatial correlations in its Chebyshev GCN based hidden layers, weights the extracted features in its dense layer and produces the binary flag in its output layer. Note that while the input layer has two channels, the CGCN layers can have multiple channels.

Although powerful, those spectral filters are computationally complex and spatially not localized due to the forward and inverse GFT operations. To reduce their complexity and make them localized, Chebyshev convolutional graph filters are proposed in [22]. Chebyshev polynomial of the first kind $T_k(x)$ with the order K can be computed by a recursion as follows:

$$T_k(x) = 2xT_{k-1}(x) - T_{k-2}(x), \quad (5)$$

where $T_0(x) = 1$ and $T_1(x) = x$ [23]. Similarly, a filter g_θ can be computed by Chebyshev polynomial approximation, T_k , up to order $K-1$. In this case, g_θ can filter \mathbf{x} using the following equation:

$$\mathbf{y} = g_\theta *_{\mathcal{G}} \mathbf{x} = \sum_{k=0}^{K-1} \theta_k T_k(\tilde{\mathbf{L}}) \mathbf{x}, \quad (6)$$

where $\theta \in \mathbb{R}^K$ is a vector of Chebyshev coefficients, and $T_k(\tilde{\mathbf{L}}) \in \mathbb{R}^{n \times n}$ is the K order Chebyshev polynomial evaluated at the scaled Laplacian $\tilde{\mathbf{L}} = 2\mathbf{L}/\lambda_{max} - \mathbf{I}_n$. Slightly changing notation, \mathbf{y} can be calculated by:

$$\mathbf{y} = \sum_{k=0}^{K-1} \theta_k \bar{\mathbf{x}}_k \quad (7)$$

where $\bar{\mathbf{x}}_0 = \mathbf{x}$, $\bar{\mathbf{x}}_1 = \tilde{\mathbf{L}}\mathbf{x}$, and $\bar{\mathbf{x}}_k$ is computed recursively by:

$$\bar{\mathbf{x}}_k = 2\tilde{\mathbf{L}}\bar{\mathbf{x}}_{k-1} - \bar{\mathbf{x}}_{k-2}. \quad (8)$$

Note that Chebyshev polynomial approximation makes g_θ K -localized and reduces its computational complexity from $\mathcal{O}(n^2)$ to $\mathcal{O}(K|\mathcal{E}|)$. Therefore, Chebyshev Graph Convolutional operation can be effectively employed to capture the spatial correlations of the power grid data. More details can be found in [21], [22].

B. Architecture of the Proposed Detector

The architecture of the proposed CGCN-based cyberattack detector is depicted in Fig. 1 where the model inputs/outputs and hidden layers are outlined with dashed and solid blocks, respectively. Due to the fact that $P_i + jQ_i = \sum_{k \in \Omega_i} P_{ik} + jQ_{ik}$, node values can be used to represent branch values as summation in their corresponding set of buses connected to them. Therefore, we only employ P_i and Q_i values to feed the proposed model. The model consists of L hidden Chebyshev

graph convolutional layers for spatial feature extraction and one dense layer for predicting the probability of the input sample being attacked. In this multilayer architecture, the input, $\mathbf{X}^{l-1} \in \mathbb{R}^{n \times c_{l-1}}$, and output, $\mathbf{X}^l \in \mathbb{R}^{n \times c_l}$, of each CGCN layer are related by equation (9).

$$\mathbf{X}^l = \text{ReLU}(\theta^l *_{\mathcal{G}} \mathbf{X}^{l-1} + \mathbf{b}^l), \quad (9)$$

where ReLU is rectified linear unit activation function, $\theta^l \in \mathbb{R}^{K \times c_{l-1} \times c_l}$ is unknown trainable Chebyshev coefficients, $\mathbf{b}^l \in \mathbb{R}^{c_l}$ is bias term of the layer l , and c_l is the number of channels in layer l for $1 \leq l \leq L$. Dense layer, on the contrary, gives y in the classical feed-forward neural network fashion by:

$$y = \sigma(\mathbf{W}^L \mathbf{X}^L + \mathbf{b}^L) \quad (10)$$

where $\mathbf{W}^L \in \mathbb{R}^{n \times c_L}$ is feature weights, $\mathbf{b}^L \in \mathbb{R}$ is the bias term and σ is the nonlinear sigmoid activation operation.

IV. NUMERICAL EXPERIMENTS & DISCUSSIONS

A. Dataset Generation

Due to the privacy reasons, there is no publicly available dataset for cyberattack detection, therefore, we generate a synthetic dataset. As a first step, for each t in $1 \leq t \leq 36000$, we scale load and generation values of each bus in the 2848-bus test system [24] by a uniform random value between 0.8 and 1.2; run AC power flow algorithms [25]; and save power measurements after adding 1% noise to them to mimic the timely behavior of the grid. Then, to simulate the cyberattacks, we implement data scale attacks (A_s) [26] and distribution-based attacks (A_d) [27] as of two frequently used cyberattack generation algorithms. Scale attacks multiply the original measurement with a number sampled from a uniform distribution between 0.9 and 1.1. In contrast, distribution-based attacks replace it with a value drawn from the Gaussian distribution satisfying the same mean and variance with the original measurements.

B. Model Training

We scale the dataset with the normal scaler for faster training, and split it into three sections to use 4/6 of them for training, 1/6 of them for validation, and 1/6 of them for testing. The number of samples in each split is given in Table I where we keep the number of attacked samples equal with

the number of unattacked samples in each split for a balanced classification problem. Each sample contains P_i , and Q_i as input features and a binary output label y to indicate the presence of the attack.

TABLE I
NUMBER OF SAMPLES IN EACH SPLIT.

split	non-attacked	A_d	A_s	total
train	12000	6000	6000	24000
validation	3000	1500	1500	6000
test	3000	1500	1500	6000

We utilize the binary cross-entropy loss function in (11) to compute all unknown parameters of the model represented with W_θ , by an end-to-end training process of N training samples.

$$L(\hat{y}, W_\theta) = \frac{-1}{N} \sum_{n=1}^N y_i \log(\hat{y}_i) + (1 - y_i) \log(1 - \hat{y}_i), \quad (11)$$

We feed samples into the model as mini batches having 2^8 samples in 2^8 maximum epoch. Moreover, we tolerate 16 epoch without any improvement in the validation set's cross entropy loss, otherwise we apply early stopping in order to avoid overfitting. We run our implementations on Intel i9-8950 HK CPU 2.90GHz with NVIDIA GeForce RTX 2070 GPU using Python 3.8 and Tensorflow 2.2 [28].

We also implement other existing deep learning based architectures in the literature such as FCN [5], RNN [6], and CNN [7] to compare the proposed CGNN-based architecture with as we do not have access to the dataset of corresponding works. For a fair comparison, we optimize the models' hyperparameters such as the number of hidden layers $\mathcal{L} = \{1, 2, 3, 4, 5\}$, the number of units $\mathcal{U} = \{8, 16, 32, 64, 128\}$, and the size of the filters $\mathcal{K} = \{3, 5, 7, 9\}$ using grid search. Similar to the proposed model, we train the detectors on the training split and tune their hyperparameters on the validation split. Table II summarizes the optimized model hyperparameters for each model.

TABLE II
OPTIMIZED MODEL HYPER-PARAMETERS.

parameter	FCN	RNN	CNN	CGCN
\mathcal{L}	4	4	3	4
\mathcal{U}	64	32	32	32
\mathcal{K}	-	-	5	5

C. Detection Results

We evaluate the model performance by the detection rate $DR = \frac{TP}{TP+FN}$ and false alarm rate $FA = \frac{FP}{FP+TN}$ where TP , FP , TN , and FN denote true positives, false positives, true negatives, and false negatives, respectively. Fig 2 presents the detection results of each model for the 2848 bus test system. Clearly, FCN falls behind other models since it has the lowest DR with 55.06% and highest FA with 62.5%.

RNN performs better than FCN with 71.19% DR and 22.43% DR . Compared to the non-convolutional architectures, i.e., FCN and RNN, the convolutional architectures, i.e., CNN and CGCN, give better results. Additionally, CGNN surpasses CNN by 7.86% in DR and 9.67% in FA .

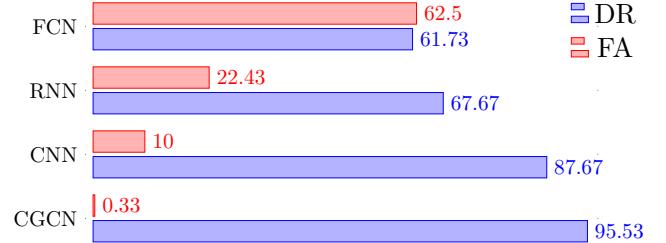


Fig. 2. Detection results in terms of DR and FA percentages.

Our experiments indicate the importance of architectural choices on the models' detection performances. For instance, FCN falls short since it ignores the locality of features and overfits to the training data. RNN, on the contrary, does not yield convenient results due to the fact that structure of power grid data do not fit well into sequence type recurrent relations. Compared to FCN and RNN, CNN gives better results since it can capture the temporal or spatial correlations of the input data in an Euclidean space in which local features can be expressed linearly. Except some trivial grids, the spatial relationship of the power grid measurements can not be fully modeled in an Euclidean space due to its graph structure. In fact, power grid data needs topology-aware architectures such as CGCN to better exploit its spatial correlations.

D. Detection Times

Detection time of a detector can be highly critical in a practical application since PSSE outcome is directly fed into various time sensitive Energy Management System (EMS) blocks including contingency and reliability analysis, load and price forecasting, and economic dispatch processes [29]. To compare the detection time of different algorithms, we measure the elapsed time during the model's detection process for each sample in the test set and tabulate the mean values in Table III.

TABLE III
MODELS' DETECTION TIMES IN MILLISECONDS.

FCN	RNN	CNN	CGCN
1.33	1125.66	3.54	3.25

As can be seen from Table III, RNN's detection time is not acceptable for real time application since it takes more than a second to respond. FCN, in contrast, yields the best detection delay with only 1.33 ms. Yet, its unsatisfactory DR and FA confine its suitability for real time application. CNN and CGCN give acceptable delays for a practical scenario with 3.54 and 3.25 ms detection times, respectively. Besides, CGCN

provides better results in terms of detection performance and delay.

V. CONCLUSION

Modern power grids are vulnerable to cyberattacks due to their highly complex and integrated cyber-physical networks. Although a number of solutions have been proposed to detect those cyberattacks, most of the studies have disregarded the inherent topology of the power grid and used small test systems to verify their algorithms. To address these issues and detect cyberattacks in large scale AC power grids, we propose a deep learning model that employs Graph Convolutional Networks in its hidden layers to better capture power grid measurements' spatial correlations. It is numerically verified on a large-scale power grid with 2848 buses that the proposed detector outperforms state-of-the-art model by 7.86% and 9.67% in false alarm rate and detection rate, respectively.

ACKNOWLEDGMENT

This work was supported by NSF under Award Number 1808064.

REFERENCES

- [1] K. R. Davis, K. L. Morrow, R. Bobba, and E. Heine, "Power flow cyber attacks and perturbation-based defense," in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2012, pp. 342–347.
- [2] G. B. Giannakis, V. Kekatos, N. Gatsis, S.-J. Kim, H. Zhu, and B. F. Wollenberg, "Monitoring and optimization for power grids: A signal processing perspective," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 107–128, 2013.
- [3] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2016.
- [4] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2218–2234, 2019.
- [5] K. Vimalkumar and N. Radhika, "A big data framework for intrusion detection in smart grids using apache spark," in *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. IEEE, 2017, pp. 198–204.
- [6] S. Binna, S. R. Kuppannagari, D. Engel, and V. K. Prasanna, "Subset level detection of false data injection attacks in smart grids," in *2018 IEEE Conference on Technologies for Sustainability (SusTech)*. IEEE, 2018, pp. 1–7.
- [7] M. Lu, L. Wang, Z. Cao, Y. Zhao, and X. Sui, "False data injection attacks detection on power systems with convolutional neural network," in *Journal of Physics: Conference Series*, vol. 1633, no. 1. IOP Publishing, 2020, p. 012134.
- [8] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *nature*, vol. 521, no. 7553, pp. 436–444, 2015.
- [9] E. Drayer and T. Routhenberg, "Detection of false data injection attacks in smart grids based on graph signal processing," *IEEE Systems Journal*, 2019.
- [10] R. Ramakrishna and A. Scaglione, "Detection of false data injection attack using graph signal processing for the power grid," in *2019 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*. IEEE, 2019, pp. 1–5.
- [11] D. Owerko, F. Gama, and A. Ribeiro, "Optimal power flow using graph neural networks," in *ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2020, pp. 5930–5934.
- [12] O. Boyaci, A. Umunnakwe, A. Sahu, M. R. Narimani, M. Ismail, K. R. Davis, and E. Serpedin, "Graph neural networks based detection of stealth false data injection attacks in smart grids," *IEEE Systems Journal*, pp. 1–12, 2021.
- [13] O. Boyaci, M. R. Narimani, K. Davis, M. Ismail, T. J. Overbye, and E. Serpedin, "Joint detection and localization of stealth false data injection attacks in smart grids using graph neural networks," *IEEE Transactions on Smart Grid*, pp. 1–1, 2021.
- [14] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 198–207, 2015.
- [15] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 612–621, 2014.
- [16] J. Duan, W. Zeng, and M.-Y. Chow, "Resilient distributed dc optimal power flow against data integrity attack," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 3543–3552, 2016.
- [17] M. N. Kurt, Y. Yilmaz, and X. Wang, "Real-time detection of hybrid and stealthy cyber-attacks in smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 498–513, 2018.
- [18] ———, "Distributed quickest detection of cyber-attacks in smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2015–2030, 2018.
- [19] J. Hao, E. Kang, J. Sun, Z. Wang, Z. Meng, X. Li, and Z. Ming, "An adaptive markov strategy for defending smart grid false data injection from malicious attackers," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2398–2408, 2016.
- [20] E. M. Ferragut, J. Laska, M. M. Olama, and O. Ozmen, "Real-time cyber-physical false data attack detection in smart grids using neural networks," in *2017 International Conference on Computational Science and Computational Intelligence (CSCI)*. IEEE, 2017, pp. 1–6.
- [21] A. Ortega, P. Frossard, J. Kovačević, J. M. Moura, and P. Vandergheynst, "Graph signal processing: Overview, challenges, and applications," *Proceedings of the IEEE*, vol. 106, no. 5, pp. 808–828, 2018.
- [22] M. Defferrard, X. Bresson, and P. Vandergheynst, "Convolutional neural networks on graphs with fast localized spectral filtering," in *Proceedings of the 30th International Conference on Neural Information Processing Systems*. Red Hook, NY, USA: Curran Associates Inc., 2016, pp. 3844–3852.
- [23] J. C. Mason and D. C. Handscomb, *Chebyshev polynomials*. CRC press, 2002.
- [24] C. Josz, S. Flisicounakis, J. Maeght, and P. Panciatici, "Ac power flow data in matpower and qcqp format: itesla, rte snapshots, and pegas," *arXiv preprint arXiv:1603.01533*, 2016.
- [25] L. Thurner, A. Scheidler, F. Schäfer, J.-H. Menke, J. Dollichon, F. Meier, S. Meinecke, and M. Braun, "pandapower - an open-source python tool for convenient modeling, analysis, and optimization of electric power systems," *IEEE Transactions on Power Systems*, vol. 33, no. 6, pp. 6510–6521, 2018.
- [26] A. Jevtic, F. Zhang, Q. Li, and M. Ilic, "Physics-and learning-based detection and localization of false data injections in automatic generation control," *IFAC-PapersOnLine*, vol. 51, no. 28, pp. 702–707, 2018.
- [27] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE transactions on neural networks and learning systems*, vol. 27, no. 8, pp. 1773–1786, 2015.
- [28] M. Abadi, P. Barham, J. Chen, Z. Chen, A. Davis, J. Dean, M. Devin, S. Ghemawat, G. Irving, M. Isard *et al.*, "Tensorflow: A system for large-scale machine learning," in *12th {USENIX} symposium on operating systems design and implementation ({OSDI} 16)*, 2016, pp. 265–283.
- [29] A. Abur and A. Expósito, *Power System State Estimation: Theory and Implementation*, ser. Power Engineering (Willis). CRC Press, 2004.