Locational Detection of False Data Injection Attacks in the Edge Space via Hodge Graph Neural Network for Smart Grids

Wei Xia, Yan Li, Lisha Yu, and Deming He

***Abstract*—Recently, the emerging False Data Injection Attacks (FDIAs), one of the major cybersecurity threats, have been severely threatening smart grids, since FDIAs could bypass conventional bad data detectors to disrupt power system operations. To maintain the security of power systems, it is critical to develop efficient locational detectors for FDIAs. However, designing FDIA detectors that could model the inherent underlying graph structures of smart grids and spatially correlated measurement data residing on both branches and buses such that FDIAs in the *edge space* could be detected and located, remains an open problem. In this work, we propose an alternative graph representation for smart grids, regarding both the power flows on branches and power injections on buses, such that we could simultaneously process these data in the edge space. We propose a Hodge Aggregation Graph Neural Network (AGNN)-based FDIA detector, leveraging the Hodge theory and exploiting the Hodge Laplacian into the AGNN. We further develop a Hodge Aggregation Graph Attention Network (AGAT)-based FDIA detector to enhance the locational detection performance of the Hodge AGNN-based detector, by utilizing the graph attention mechanism. Illustrative simulation results demonstrate the superior locational detection performance of the proposed detectors, compared to the other state-of-the-art FDIA detectors.**

***Index Terms*—Smart grids, cyber security, situational awareness, false data injection attacks (FDIAs), graph signal processing (GSP), Hodge theory, graph neural network (GNN), edge space.**

Nomenclature

Acronyms

AGAT	Aggregation Graph Attention Network.
AGNN	Aggregation Graph Neural Network.
CNN	Convolutional Neural Network.
DC	Direct Current.
DT	Decision Tree.
FDIAs	False Data Injection Attacks.
GCN	Graph Convolutional Network.
GNB	Gaussian Naive Bayes.
GNN	Graph Neural Network.
GSP	Graph Signal Processing.
KNN	K-Nearest Neighbor.
MLP	Multi-layer Perceptron.
SVM	Support Vector Machine.

Symbols

$\mathcal{G}$, $\mathcal{G}_\mathrm{e}$	Original and reconstruction graphs.
z_o, $\boldsymbol{z}$	Physical measurements in the absence of FDIAs and in the presence of FDIAs.
E, E_e	Number of edges of $\mathcal{G}$ and $\mathcal{G}_\mathrm{e}$.
M	Number of meters.
N	Number of nodes of $\mathcal{G}$.
$\boldsymbol{B}$	Incidence matrix of $\mathcal{G}_\mathrm{e}$.
$\boldsymbol{L}_1$	Hodge Laplacian.
$\boldsymbol{O}_\mathrm{s}^{(d)}$	Output of the dth attention mechanism.
$\boldsymbol{O}_\mathrm{c}$	Output of the CNN layer.
$\boldsymbol{O}_\mathrm{s}$	Output of the Hodge aggregation layer.
$\boldsymbol{S}$	Graph shift operator.
$\boldsymbol{W}_\mathrm{D}$	Trainable matrix.
$\boldsymbol{h}_j$	The jth convolution filter.
$\boldsymbol{o}_\mathrm{f}$	Output of the flatten layer.
$\boldsymbol{w}_\mathrm{a}$, $\boldsymbol{m}$	Trainable parameter vectors.
$\boldsymbol{x}$	System state in the absence of FDIAs.
$\boldsymbol{y}_\mathrm{o}$	Predicted result.
$\delta_{i,j}$	Attention coefficient.
$\hat{\boldsymbol{y}}$	Output of the HodgeNet-based detectors.
$\hat{\boldsymbol{x}}_\mathrm{o}$	System state estimate in the absence of FDIAs.
λ_max	Largest eigenvalue of $\boldsymbol{B}^\mathrm{T}\boldsymbol{B}$.
$\mathcal{E}$, $\mathcal{E}_\mathrm{e}$	Sets of edges of $\mathcal{G}$ and $\mathcal{G}_\mathrm{e}$.
$\mathcal{E}_\mathrm{e}^{(M)}$	Observed edge set.
$\mathcal{N}_i^\mathrm{e}$	Neighborhood of edge i of $\mathcal{G}_\mathrm{e}$.
$\mathcal{V}$, $\mathcal{V}_\mathrm{e}$	Sets of nodes of $\mathcal{G}$ and $\mathcal{G}_\mathrm{e}$.
$\tilde{\boldsymbol{f}}$, $\boldsymbol{f}$	Flow signals on $\mathcal{G}$ and $\mathcal{G}_\mathrm{e}$.
ς_i	Scaling parameter for bus i.

Manuscript received 27 June 2023; revised 10 December 2023 and 29 March 2024; accepted 13 April 2024. Date of publication 16 April 2024; date of current version 23 August 2024. This work was supported in part by the National Natural Science Foundation of China under Grant 61871104. Paper no. TSG-00954-2023. *(Corresponding author: Wei Xia.)*

Wei Xia is with the School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China, and also with the School of Computer Science and Technology and the School of Cyberspace Security, Xinjiang University, Ürümqi 830046, China (e-mail: wx@uestc.edu.cn).

Yan Li and Deming He are with the School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: huohuol@std.uestc.edu.cn; demingh@std.uestc.edu.cn).

Lisha Yu was with the School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China. She is now with the Department of Protocol Product Center, China Satellite Network Application Company Ltd., Chongqing 401120, China (e-mail: lishayu_1998@163.com).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSG.2024.3389948.

Digital Object Identifier 10.1109/TSG.2024.3389948

I. Introduction

THE emerging Internet of Things (IoTs) has been extensively applied to medical, industrial control, communication, energy systems [1], transportation as well as precarious infrastructures [2], [3]. However, potential threats of cyber-attacks launched by malicious attackers leveraging technological vulnerabilities would endanger critical infrastructures such as smart grids [3], [4]. Thus, operators of smart grids would generally expect to make appropriate decisions for the sake of security and stability of power systems, via monitoring power system states with Supervisory Control and Data Acquisition (SCADA) systems, Phasor Measurements Units (PMUs), or Wide-Area Monitoring Systems (WAMSs) [5], [6], [7].

False Data Injection Attacks (FDIAs), as one of the major cyber-attacks on smart grids, have been posing severe threats to public security, owing to the in-depth integration of physical and network systems [8], [9], [10], [11]. Specifically, by injecting false data into physical measurements (consisting of power flows on branches and power injections on buses) of smart grids, attackers would launch FDIAs which can bypass conventional Bad Data Detectors (BDDs) to corrupt the power system state estimation [8], [9], [10], [11]. Unaware of the presence of FDIAs, smart grid operators would perform inappropriate actions according to the compromised system state estimates, resulting in probable overloading or even physical damage to smart grids.[1]

Research regarding the detection of FDIAs in smart grids has recently been arousing increasing interests [15], [16], [17], [18], [19], [20], [21], [22], [23], [24]. For instance, a comprehensive top-down scheme based on the Decision Tree (DT) and Support Vector Machine (SVM) [15] has been experimentally demonstrated to be capable of detecting FDIAs in smart grids with the accuracy of 92.5% and the false positive rate as low as 5.12% with the energy consumption dataset for homes in the USA [15]. The detection accuracy of the DT-based FDIA detector [16] is observed to be 92.25% and 95.13% respectively for the IEEE 14-bus and 39-bus test grids generated by Pandapower, which has been extensively utilized to facilitate the validation of the efficacy of FDIA detectors in detecting false data injection attacks on power systems [16], [17], [18], [19], [20], [21], [22], [23], [24]. With the supervised learning over labeled data utilized to train a distributed SVM, the efficacy of a statistics-based FDIA detector has been verified for the IEEE standard test grid [17]. The detection performance of the FDIA detectors based on the SVM and K-Nearest Neighbor (KNN) have also been evaluated for the IEEE 30-bus test grid [18]. Moreover, the superior detection performance of the FDIA detector based on the Multi-layer Perceptron (MLP) using the residuals of the system state estimate has been experimentally demonstrated for the IEEE 13-bus test grid [19]. Additionally, superior detection performance of a deep learning-based FDIA detector that concatenates a Convolutional Neural Network (CNN) with a standard BDD has been validated for the IEEE 14-bus test grid [20].

More recently, owing to the merit of real-time data acquisition by edge computing, a Classification of Predicted Residuals (CPRs)-based FDIA detector has been developed by predicting the measurements and classifying the prediction residuals [25]. By integrating the autoencoders into an advanced generative adversarial network framework, FDIAs can be detected with a semi-supervised deep learning approach, whose accuracy and efficiency are validated with a case study on the IEEE 13-bus test grid [22]. In addition, inspired by the federated learning, an FDIA detection method based on secure federated deep learning is proposed by combining Transformer, federated learning and Paillier cryptosystem [23]. Other related works on FDIA detection for smart grids could be referred to [21].

Intuitively, in view of the connectivities and interactions of smart grids, the irregular topologies of power systems can be generally modeled as graphs [26], with each grid bus and branch abstracted as a vertex (node) and an edge, respectively. It is thus promising to enhance the detection performance by exploiting the underlying graph structure of smart grids and leveraging the emerging Graph Signal Processing (GSP) methodology. Recently, modeling system states (voltage phasors) or power injections on buses as signals supported on nodes, various FDIA detectors leveraging GSP have been developed [26], [27], [28], [29], [30], [31], [32]. For instance, the FDIA detector exploiting graph filters has been experimentally demonstrated to be effective in detecting FDIAs [27], [28]. Based on the GSP methodology, an FDIA detector with subspace projection [30] and an FDIA detector utilizing tools from blind community detection [31] have been proposed to detect FDIAs efficiently. The recently proposed Grid-GSP framework [26] provides a general perspective to leverage the GSP methodology for analyzing the system states of smart grids. Additionally, based on the GSP methodology, via subspace projection, the FDIA detector incorporating the quasi-optimal PMU placement strategy could also detect FDIAs with a high detection probability [32].

Nevertheless, the aforementioned GSP-based FDIA detectors [27], [28], [31], [32] could only detect the presence of FDIAs, but are incapable of simultaneously locating the attacked meters in a power system. Deep learning techniques incorporating the GSP methodology, namely, Graph Neural Networks (GNNs), such as the Graph Convolutional Network (GCN) [33] and Hodge Aggregation GNN (AGNN) [34], have been generalized to process the data supported on nodes of graphs. Specifically, the superiority of the GNN has been demonstrated in locating FDIAs in smart grids, via nodal feature propagation and aggregation [29]. The GCN [33] has recently been applied to develop the FDIA detectors with enhanced detection performance [29]. Based on the Graph Convolutional Attention Network (GCAT), an FDIA detector has been proposed for the locational detection of FDIAs, by leveraging the graph attention mechanism, which could elastically assign the graph shift operators, to enhance the locational detection performance [35].

The aforementioned FDIA detectors [27], [28], [29], [31], [32], [35] utilizing the inherent underlying graph structures

[1] Power systems would also malfunction owing to a fault, which is usually associated with an abnormal electric current exceeding normal operating conditions [8], [12]. Fault detection [13], [14] is out of the scope of this work.

of smart grids, can only process the data associated with nodes of graphs, or, the data in the *node space*. However, these detectors generally could not deal with power flows on branches (edges) of practical smart grids [8], [9], [11], which could be readily modeled as the edge data in the *edge space* [36], [37].

Recently, various problems associated with the data supported on the edges of graphs have been successfully tackled with the methods incorporating the Hodge theory, with the graph (or network) modeled as a simplicial complex [36], [37], [38], [39], [40], [41], [42]. For example, with edge space data, a class of edge filters based on the Hodge Laplacian is introduced to smooth and denoise flows, by optimizing the regularized problems [36]. Random walk algorithm in the node space has been generalized to the edge space, with the normalized Hodge Laplacian [37]. Moreover, based on the GNN with the Hodge Laplacian, the HodgeNet is proposed to solve the problems of flow interpolation and source localization [38].

Intuitively, by exploiting *the spatial correlation of both buses and branches* in the smart grids, the locational detection performance of the detectors can be further enhanced, as attacks could be potentially launched on the meter(s)/branches of smart grids. Nevertheless, to the best of the authors' knowledge, there is a lack of investigation on FDIA detection for smart grids in the edge space, by using data residing on edges of graphs and exploiting the underlying graph structures of smart grids, despite its potential practical importance. Further, there is also a lack of research on the graph modeling methodology such that data supported both on the branches and buses of smart grids can be processed simultaneously in the edge space. As attackers could only launch attacks on partial meters/branches due to the limit of the available knowledge and resources [8], power system operators would expect to detect and locate those compromised meter(s)/branch(es), which is the scope of this work. The FDIA detection methodology could be potentially applied to detecting and locating FDIAs on other IoTs such as intelligent transportation, health monitoring, and energy management, etc.

In this paper, utilizing the underlying graph structures of smart grids, we consider not only detecting but also locating FDIAs on smart grids. Considering the property of power data in smart grids, we first develop a graph representation for smart grids such that we could simultaneously process the data residing on both branches and buses in the edge space. Exploiting the underlying graph topologies of smart grids, we develop a Hodge AGNN-based FDIA detector, with the integration of the AGNN and the Hodge Laplacian. Regarding the weighted graph, we further propose a Hodge Aggregation Graph Attention Network (AGAT)-based FDIA detector, incorporating the graph attention mechanism into the Hodge AGNN-based FDIA detector. Illustrative simulation results validate the superior performance of both the proposed Hodge AGNN-based and Hodge AGAT-based FDIA detectors, compared to the other state-of-the-art FDIA detectors. It is also experimentally demonstrated that the Hodge AGAT-based FDIA detector outperforms the Hodge AGNN-based FDIA detector, whereas both proposed detectors outperform the other state-of-the-art competitors when meters are only deployed at partial edges.

The main contributions of this work are summarized as follows.

- Regarding both the power flows on branches and power injections on buses and taking their physical implication into account, we propose an alternative graph representation of smart grids, such that we could process simultaneously the data residing on both branches and buses in the edge space.
- We propose a Hodge AGNN-based FDIA detector modeling the inherent underlying graph structures of smart grids, by incorporating the Hodge Laplacian into the AGNN.
- Considering the weighted graph, we further exploit the graph attention mechanism to adapt the Hodge Laplacian in the Hodge AGNN. We accordingly develop a Hodge AGAT-based FDIA detector, whose performance enhancement compared to the Hodge AGNN-based FDIA detector is experimentally validated.

Notation: The set of real numbers is denoted by $\mathbb{R}$. Scalars, vectors and matrices are given by lower-case letters (a), lower-case boldface letters ($\boldsymbol{a}$) and upper-case boldface letters ($\boldsymbol{A}$), respectively. The ith entry of the vector $\boldsymbol{a}$ is denoted by $[\boldsymbol{a}]_i$, the (i,j)th entry of the matrix $\boldsymbol{A}$ is denoted by $[\boldsymbol{A}]_{i,j}$, and the ith row of $\boldsymbol{A}$ is denoted by $[\boldsymbol{A}]_{i,:}$. The transpose of the matrix or vector is denoted by $(\cdot)^{\mathrm{T}}$, and the inverse of the matrix is represented as $(\cdot)^{-1}$. $\|\cdot\|_2$ and $\|\cdot\|_\infty$ denote the l_2-norm and infinite norm of the vector, respectively. $\boldsymbol{I}_M$ and $\mathbf{1}$ denote respectively $M \times M$ identity matrix and the all-ones column vector with a matching dimension. $\mathbf{0}$ denotes the all-zeros column vector with a matching dimension. $\|$ represents the concatenation operation.

II. Problem Formulation

A. Reconstruction Graph Representation of Smart Grids

In smart grids, the connection of various interconnected power facilities (e.g., loads, generators and distribution substation) can be abstracted to corresponding irregular topologies. Thus, we herein model an N-bus power system as an undirected graph $\mathcal{G} \triangleq (\mathcal{V}, \mathcal{E})$ [27], [28], [29], where $\mathcal{V} = \{1, 2, \ldots, N\}$ represents the bus (node) set composed of load or generator buses, and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ represents the branch (edge) set composed of branches connecting two buses. We indicate the cardinalities of the node and edge sets as $|\mathcal{V}| = N$ and $|\mathcal{E}| = E$, respectively. Additionally, following the definition of the adjacent k-simplices [41], [43], we say two edges are adjacent if they have a common node. For each edge i, we define its neighborhood $\mathcal{N}_i^{\mathrm{e}}$ as the set of its adjacent edges (including the edge i itself). We consider herein the edge space data [36], [38], i.e., the data residing on the edges of a graph. We herein define the flow signal $\tilde{\boldsymbol{f}} \in \mathbb{R}^E$ on the edges of the original graph $\mathcal{G}$, and each entry of $\tilde{\boldsymbol{f}}$ corresponds to the power measurement on the corresponding branch.

It is noteworthy that it is generally necessary to simultaneously process data supported on either the nodes or the edges of the graph $\mathcal{G}$, as power measurements could be on

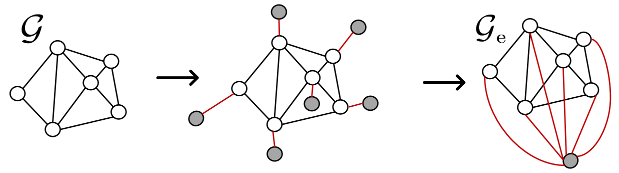


Fig. 1. The reconstruction process of the original graph $\mathcal{G}$.

either the branches or the buses of smart grids [8], [9], [11]. Nevertheless, based on the original graph $\mathcal{G}$, we cannot analyze the node space data residing on the edges of a graph, as we consider fulfilling tasks in smart grids in the edge space. Without loss of generality, to simultaneously process data on both branches and buses, we herein propose an alternative graph representation of smart grids, by reconstructing the original graph $\mathcal{G}$.

Specifically, to map the node space data to the data associated with the edges, we first add N imaginary nodes (in gray) to the original graph $\mathcal{G}$. Each imaginary node is connected with one different node in $\mathcal{G}$ by an edge (in red). The data residing on each node in the original graph $\mathcal{G}$ is mapped to those residing on the red edge connected to the corresponding bus, and thus all the data (including those on the buses and on the branches) are now in the edge space. Then, we further consider merging all the imaginary nodes into one imaginary node, and the resulting reconstruction graph $\mathcal{G}_\mathrm{e} = (\mathcal{V}_\mathrm{e}, \mathcal{E}_\mathrm{e})$ is shown in Fig. 1. It is noting that the sum of the power values on the edges connected to each node in the reconstruction graph $\mathcal{G}_\mathrm{e}$ equals zero. We denote the node and edge sets of the reconstruction graph $\mathcal{G}_\mathrm{e}$ as $\mathcal{V}_\mathrm{e} = \{1, 2, \ldots, N, N+1\}$ and $\mathcal{E}_\mathrm{e} = \{\epsilon_j\}_{j=1}^{E_\mathrm{e}} \subseteq \mathcal{V}_\mathrm{e} \times \mathcal{V}_\mathrm{e}$ with $|\mathcal{E}_\mathrm{e}| = E_\mathrm{e} = E + N$, respectively. The flow signal in the reconstruction graph $\mathcal{G}_\mathrm{e}$ can be represented as $\boldsymbol{f} \in \mathbb{R}^{E_\mathrm{e}}$, which consists of data on both all the buses and branches in the smart grid. Notice that the flow signal $\boldsymbol{f}$ in the reconstruction graph $\mathcal{G}_\mathrm{e}$ satisfies $[\boldsymbol{f}]_i = [\tilde{\boldsymbol{f}}]_i, i = 1, 2, \ldots, E$. It is noteworthy that the graph reconstruction method can be directly applied to lossy power systems, as the sum of the power values on all the nodes and edges in either lossless or lossy power systems equals zero.

The edges of the reconstruction graph $\mathcal{G}_\mathrm{e}$ can be conveniently collected as the entries of the adjacency matrix $\boldsymbol{A} \in \mathbb{R}^{(N+1)\times(N+1)}$ [27], [28], [29], where $\boldsymbol{A}_{i,p} \neq 0$ for all $\epsilon_j = (i, p) \in \mathcal{E}_\mathrm{e}$, and $\boldsymbol{A}_{i,p} = 0$, otherwise. As an alternative way to encode a graph, the node-to-edge incidence matrix $\boldsymbol{B} \in \mathbb{R}^{(N+1)\times E_\mathrm{e}}$ could describe the relationships between nodes and edges [36], [40], [41]. Specifically, with the same indexing of $\mathcal{V}_\mathrm{e}$ and a labeling of $\mathcal{E}_\mathrm{e}$ with $\{\epsilon_j\}_{j=1}^{E_\mathrm{e}}$,

$$[\boldsymbol{B}]_{i,j} = \begin{cases} c_{i,j}, & \epsilon_j = (i,p) \text{ for some } p \in \mathcal{V}_\mathrm{e}, \\ -c_{i,j}, & \epsilon_j = (p,i) \text{ for some } p \in \mathcal{V}_\mathrm{e}, \\ 0, & \text{otherwise}, \end{cases} \tag{1}$$

assigns an inherent direction to each edge ϵ_j. Without loss of generality, we stipulate that the flow signal on ϵ_j leaves from node i and flows into node p if $[\boldsymbol{B}]_{i,j} > 0$, while the direction of the signal is inverse if $[\boldsymbol{B}]_{i,j} < 0$. It is noteworthy that for undirected graphs, the stipulation does not affect other graph signal processing in a meaningful way [38]. Specially, we have $c_{i,j} = 1$ for unweighted graphs [42]. For weighted graphs, $c_{i,j}$ depends on the graph shift operator $\boldsymbol{S}$ obtained through learning, and is not necessarily equal to 1.

In light of the Hodge theory, the Hodge Laplacian [40], [41], commonly defined as

$$\boldsymbol{L}_1 = \boldsymbol{B}^\mathrm{T}\boldsymbol{B} \in \mathbb{R}^{E_\mathrm{e}\times E_\mathrm{e}} \tag{2}$$

is an alternative graph shift operator $\boldsymbol{S} \in \mathbb{R}^{E_\mathrm{e}\times E_\mathrm{e}}$ for flow signals in the edge space. Analogous to the graph shift operator in the node space, the graph shift operator $\boldsymbol{S}$ accounting for the local graph structure of power grids in the edge space could replace the value on each edge i with the linear combination of the values in the neighborhood $\mathcal{N}_i^\mathrm{e}$. Obviously, the sparsity and locality of the relationships among different elements of flow signal $\boldsymbol{f}$ could be captured by $\boldsymbol{L}_1$, such that the one-hop shift of the flow signal $\boldsymbol{f}$ can be represented as $\boldsymbol{L}_1\boldsymbol{f}$.

B. False Data Injection Attacks

In smart grids, the system states, which would be undermined by the FDIAs, are essential for the security and stability of power systems [5], [6]. System states of smart grids can be estimated based on either the Alternating Current (AC) or Direct Current (DC) power flow models [6]. DC power flow model with a simpler structure is more reliable, and the DC power flow model could approximate the AC power flow model. Hence, we consider herein the DC power flow model, for simplicity.

With M meters in the N-bus power system, the physical measurement $z_\mathrm{o} = [z_1, z_2, \ldots, z_M]^\mathrm{T} \in \mathbb{R}^M$ consists of the active power flows on the branches and active power injections on the buses from meters, and each entry of the system state $\boldsymbol{x} = [x_1, x_2, \ldots, x_N]^\mathrm{T} \in \mathbb{R}^N$ corresponds to the voltage phase angle of each bus. Thus, in the DC power flow model, the relationship between the physical measurement z_o and the system state $\boldsymbol{x}$ can be given by

$$z_\mathrm{o} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{e}, \tag{3}$$

where $\boldsymbol{H} \in \mathbb{R}^{M\times N}$ represents the Jacobian matrix pertinent to the topology of the power system and transmission line impedance [27], and $\boldsymbol{e} \in \mathbb{R}^M$ denotes the zero-mean additive white Gaussian noise with the covariance matrix $\boldsymbol{\Sigma} = \sigma^2\boldsymbol{I}_M$. We can obtain the optimal system state estimate

$$\hat{x}_\mathrm{o} = \left(\boldsymbol{H}^\mathrm{T}\boldsymbol{\Sigma}^{-1}\boldsymbol{H}\right)^{-1}\boldsymbol{H}^\mathrm{T}\boldsymbol{\Sigma}^{-1}z_\mathrm{o}, \tag{4}$$

by utilizing the Weighted Least Squares (WLS) criterion [6], [21], [35]

$$\min_{\boldsymbol{x}}\left\{J(\boldsymbol{x}) \triangleq (z_\mathrm{o} - \boldsymbol{H}\boldsymbol{x})^\mathrm{T}\boldsymbol{\Sigma}^{-1}(z_\mathrm{o} - \boldsymbol{H}\boldsymbol{x})\right\}, \tag{5}$$

with its convergence proof given in [44].

The system state estimation might be corrupted due to the bad data (e.g., large meter or communication error) [8]. The conventional BDDs [8] can detect the bad data through comparing the square of the l_2-norm of the measurement residual,

$$r = \left\|z_\mathrm{o} - \boldsymbol{H}\hat{\boldsymbol{x}}_\mathrm{o}\right\|_2^2 \gtrless \tau_r, \tag{6}$$

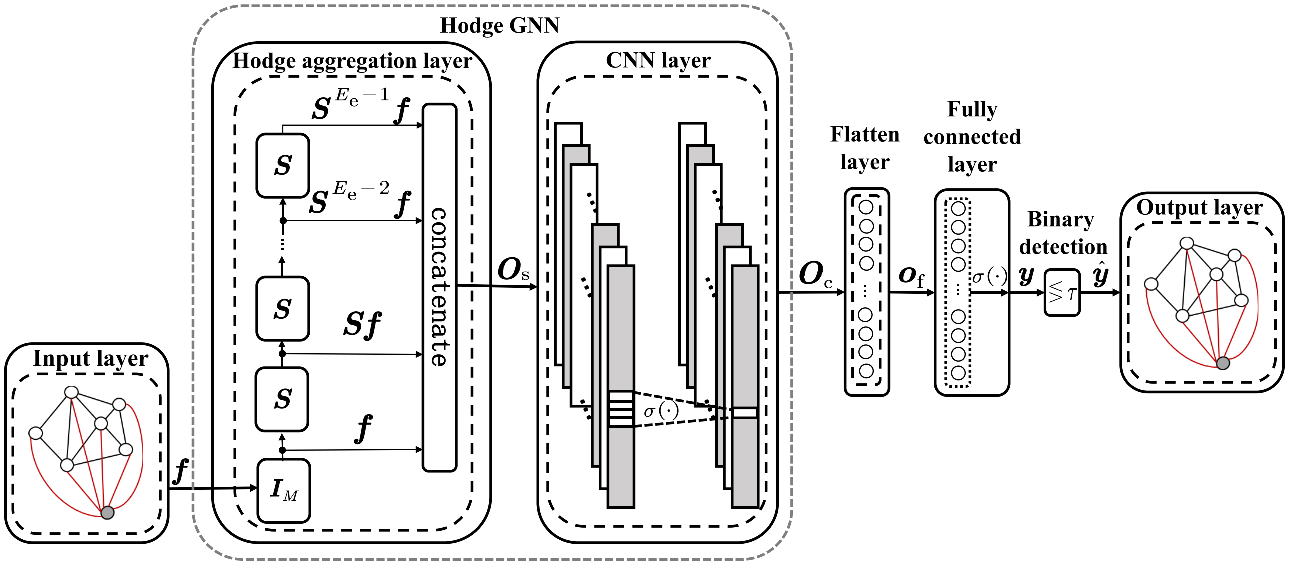


Fig. 2. The unified architecture of the HodgeNet-based detectors.

given the threshold τ_r.

On the other hand, considering the presence of FDIAs, we can rewrite the system state estimate in a unified form,

$$\hat{x} = \begin{cases} \hat{x}_o + c, & \mathcal{H}_1, \\ \hat{x}_o, & \mathcal{H}_0, \end{cases} \tag{7}$$

where the error vector $c \in \mathbb{R}^N$ is induced by FDIAs. $\mathcal{H}_0$ represents the FDIA-free hypothesis, and the alternative hypothesis $\mathcal{H}_1$ represents the presence of FDIAs. Notice that the error vector c is generally sparse, since attackers are either constrained to some specific measurement meters or limited in the resources required to compromise the meters persistently [45], [46]. Likewise, the physical measurement can be rewritten in a unified form,

$$z = \begin{cases} H(x + c) + e = z_o + a, & \mathcal{H}_1, \\ z_o, & \mathcal{H}_0, \end{cases} \tag{8}$$

where $a \in \mathbb{R}^M$ denotes the attack vector. As the measurement residual r in (6) would unchange given $a = Hc$, FDIAs could bypass the BDDs [8], [9], and thus result in probable overloading or even physical damage to smart grids.

Without loss of generality, we consider deploying M meters on all the buses and branches in smart grids, i.e., $M = N + E = E_e$. Obviously, the aforementioned flow signal f in Section II-A consists of all the physical measurements of z_o, and each entry of f represents the active power data either on the corresponding branch or injected into the related bus. In the experiment hereinafter, we also consider the practical scenario that only partial measurements obtained from $M < E_e$ meters.

In this work, based on the reconstruction graph $\mathcal{G}_e$, in smart grids, we consider not only detecting FDIAs but also locating the attacked meters in the edge space [36], [38], by analyzing the power measurement from meters and exploiting the underlying graph topology structure.

III. HodgeNet-Based Detectors

Regarding the underlying topologies of smart grids, based on the Hodge theory, we consider developing the HodgeNet-based FDIA detector architecture by incorporating the Hodge Laplacian into the AGNN, such that the meters under FDIA could be located. Furthermore, considering the weighted graph, we apply the graph attention mechanism [47] to adapt the weighted Hodge Laplacian in the Hodge AGNN, and the resulting detector is dubbed the Hodge AGAT-based FDIA detector. For convenience, the Hodge AGNN-based and Hodge AGAT-based detectors are collectively known as the HodgeNet-based detectors.

A. HodgeNet-Based FDIA Detector Architecture

The unified architecture of the HodgeNet-based detectors is illustrated in Fig. 2, and consists of the input layer, Hodge aggregation layer, CNN layer, flatten layer, fully connected layer, binary decision and output layer.

The E_e inputs of the input layer represent the power flow measurement on each branch and the power injection measurement on each bus at each time instance. With the flow signal f as the input, the Hodge aggregation layer would yield the multi-channel sequence $O_s \in \mathbb{R}^{E_e \times Q}$ via the aggregation operation, where Q denotes the feature number of the Hodge aggregation layer.

Feeding O_s into the 1-dimensional CNN would yield the output feature $O_c \in \mathbb{R}^{E_e \times F_c}$, where F_c denotes the number of output channels of the CNN. The output feature O_c would be reduced to the one-dimensional feature $o_f \in \mathbb{R}^{E_e F_c}$ via the flatten layer. Each entry of the output $y \in \mathbb{R}^{E_e}$ of the fully connected layer corresponds to the probability of the corresponding meter being attacked. Finally, with the output $\hat{y}$ of the binary decision, the HodgeNet-based detectors would determine whether each meter is under FDIA or not.

Notice that the HodgeNet-based FDIA detector can be implemented with different methods. We consider herein the Hodge aggregation layer incorporated with either Hodge AGNN or Hodge AGAT. As illustrated in Fig. 2, the architecture of the HodgeNet-based detectors consists of the Hodge aggregation layer as well as the CNN layer, followed by the conventional flatten layer, fully connected layer, binary decision, and the output layer.

B. Hodge GNN

We now consider the implementation of the Hodge GNN comprised of the Hodge aggregation and the CNN layers, utilizing the underlying graph topology of the power system.

Hodge AGNN: Regarding the flow signals in the edge space, by incorporating the normalized Hodge Laplacian [37] into the AGNN [34] (the Hodge AGNN), we correspondingly propose the Hodge AGNN-based detector.

Specifically, by shifting the flow signal and concatenating the shifted signals, we can obtain the output $\boldsymbol{O}_{\mathrm{s}}$ of the Hodge aggregation layer. The multi-channel sequence output $\boldsymbol{O}_{\mathrm{s}}$ can be given by

$$\boldsymbol{O}_{\mathrm{s}} = \left[\boldsymbol{f}, \boldsymbol{S}\boldsymbol{f}, \boldsymbol{S}^2\boldsymbol{f}, \ldots, \boldsymbol{S}^{E_{\mathrm{e}}-1}\boldsymbol{f}\right]. \tag{9}$$

We herein select the normalized Hodge Laplacian $\boldsymbol{B}^{\mathrm{T}}\boldsymbol{B}/\lambda_{\max}$ as the graph shift operator $\boldsymbol{S}$, where $\lambda_{\max}$ denotes the largest eigenvalue of $\boldsymbol{B}^{\mathrm{T}}\boldsymbol{B}$. The incidence matrix $\boldsymbol{B}$ is given by (1) with $c_{i,j} = 1$. It is noteworthy that each column i of the output $\boldsymbol{O}_{\mathrm{s}}$ represents the i-hop shift of the flow signal $\boldsymbol{f}$, $i = 0, 1, \ldots, E_{\mathrm{e}} - 1$, and each row j of the output $\boldsymbol{O}_{\mathrm{s}}$ represents the signal at the corresponding edge ϵ_j of the reconstruction graph $\mathcal{G}_{\mathrm{e}}$. Moreover, the edge labeling and orientations have no effect on the output $\boldsymbol{O}_{\mathrm{s}}$ of the Hodge aggregation layer, as demonstrated in [38], [43].

Hodge AGAT: Practically, appropriate weights of the Hodge Laplacian are essential to enhance the locational detection performance of the FDIA detector, akin to [35], and thus the weighted graph can better model the relationships between various power facilities in the power system. Regarding the weighted graph, we further apply the graph attention mechanism to learn the weighted Hodge Laplacian, also known as the Attention Laplacian [48]. Incorporating the graph attention mechanism into the Hodge AGNN, we correspondingly develop the Hodge AGAT.

In the Hodge AGAT, each entry of $\boldsymbol{L}_1$ in the Hodge aggregation layer (9) can be determined by the graph attention mechanism. Specifically, each non-zero entry of graph shift operator $\boldsymbol{S}$ can be obtained by

$$\begin{aligned}[\boldsymbol{S}]_{i,j} &= \operatorname{softmax}\left(\delta_{i,j}\right) = \frac{\exp\left(\delta_{i,j}\right)}{\sum_{j\in\mathcal{N}_i^{\mathrm{e}}} \exp\left(\delta_{i,j}\right)}, \\ &= \frac{\exp\left(\sigma\left(\left[\left[\boldsymbol{f}\boldsymbol{w}_{\mathrm{a}}\right]_{i,:} \| \left[\boldsymbol{f}\boldsymbol{w}_{\mathrm{a}}\right]_{j,:}\right]\boldsymbol{m}\right)\right)}{\sum_{j\in\mathcal{N}_i^{\mathrm{e}}} \exp\left(\sigma\left(\left[\left[\boldsymbol{f}\boldsymbol{w}_{\mathrm{a}}\right]_{i,:} \| \left[\boldsymbol{f}\boldsymbol{w}_{\mathrm{a}}\right]_{j,:}\right]\boldsymbol{m}\right)\right)}, \end{aligned} \tag{10}$$

where $\delta_{i,j}$ represents the attention coefficient, $\boldsymbol{w}_{\mathrm{a}} \in \mathbb{R}^{1\times F_{\mathrm{s}}}$ and $\boldsymbol{m} \in \mathbb{R}^{2F_{\mathrm{s}}}$ denote trainable parameter vectors, with F_{s} features in the attention mechanism. In addition, we select the PReLU function [49]

$$\operatorname{PReLu}(x) = \begin{cases} x, & \text{if } x \geq 0, \\ \alpha x, & \text{if } x < 0, \end{cases} \tag{11}$$

as the nonlinear activation function $\sigma(\cdot)$ in (10) with the trainable negative input slope parameter α initialized as 0.2. Notice that the attention coefficient $\delta_{i,j}$ only depends on the features on both edge ϵ_j and its adjacent edge ϵ_i, and represents the importance of the features on edge ϵ_i to edge ϵ_j.

We further adopt the multi-head attention mechanism [47] to improve the effectiveness of the locational detection performance of the Hodge AGAT-based detector. Here, the Hodge aggregation layer of the Hodge AGAT contains D independent attention mechanisms. The output features $\boldsymbol{O}_{\mathrm{s}}$ of the Hodge aggregation layer are obtained with the output features of D independent aggregation operations (9). Specifically, we concatenate the output features $\boldsymbol{O}_{\mathrm{s}}^{(d)}$ of the aggregation operation (9), and correspondingly obtain the output features

$$\boldsymbol{O}_{\mathrm{s}} = \|_{d=1}^{D} \boldsymbol{O}_{\mathrm{s}}^{(d)}, \tag{12}$$

with $d = 1, 2, \ldots, D$.

As the attention mechanism (10) adaptively learns the Hodge Laplacian by utilizing the features in the edge space, the performance of locational detection of the Hodge AGAT-based FDIA detector can be enhanced compared with the Hodge AGNN-based FDIA detector, as demonstrated in the illustrative simulations hereinafter.

We then apply the 1-dimensional CNN to the feature $\boldsymbol{O}_{\mathrm{s}}$, with F_{c} convolution filters $\boldsymbol{h}_j \in \mathbb{R}^{hQ}, j = 1, 2, \ldots, F_{\mathrm{c}}$, where the parameter h is adjustable for the length of each convolution filter [34], [50]. Note that $Q = E_{\mathrm{e}}$ for the Hodge AGNN-based detector and $Q = DE_{\mathrm{e}}$ for Hodge AGAT-based detector. Then, the ith feature of the jth channel in the output $\boldsymbol{O}_{\mathrm{c}}$ of the CNN layer can be given by

$$[\boldsymbol{O}_{\mathrm{c}}]_{i,j} = \sigma\left(\overline{\boldsymbol{o}}_i^{\mathrm{s}}\boldsymbol{h}_j + b_{i,j}\right), \tag{13}$$

where $\overline{\boldsymbol{o}}_i^{\mathrm{s}} = \|_{l=i}^{l=i+h-1}[\boldsymbol{O}_{\mathrm{s}}]_{l,:}$, and $b_{i,j}$ represents the bias of the corresponding entry. We select the ReLU function [49]

$$\operatorname{ReLu}(x) = \begin{cases} x, & \text{if } x \geq 0, \\ 0, & \text{if } x < 0, \end{cases} \tag{14}$$

as the activation function $\sigma(\cdot)$ in (13). Alternatively, note that benefiting from the CNN architecture, the regular convolution operation linearly relates consecutive elements of $[\boldsymbol{O}_{\mathrm{s}}]_{i,:}$ of edge ϵ_i. Moreover, since consecutive elements of $[\boldsymbol{O}_{\mathrm{s}}]_{i,:}$ reflect neighborhoods of edge ϵ_i according to the reconstruction graph, we could effectively relate the values on the adjacent edges of the edge ϵ_i by means of a regular convolution.

C. Other Operations

Next, as shown in Fig. 2, we respectively brief the specific operations of the flatten layer, fully connected layer and binary decision for both the Hodge AGNN-based and Hodge AGAT-based detectors.

The output features $\boldsymbol{O}_{\mathrm{c}}$ of the CNN layer is merged into one single vector $\boldsymbol{o}_{\mathrm{f}} \in \mathbb{R}^{E_{\mathrm{e}}F_{\mathrm{c}}}$ via the flatten layer. Then, with

```
Algorithm 1: The HodgeNet-Based Detectors
Input: Flow signal $\boldsymbol{f}$, Incidence matrix $\boldsymbol{B}$, Feature
       number $Q$, Filter parameter $h$
Output: The HodgeNet-based detector model
Obtain $\boldsymbol{O}_\mathrm{s}$ with either the Hodge AGNN or Hodge AGAT.
for each shift $i = 1$ till $Q$ do
    $\bar{\boldsymbol{o}}_i^\mathrm{s} \leftarrow \{[\boldsymbol{O}_\mathrm{s}]_{i,:}, \ldots, [\boldsymbol{O}_\mathrm{s}]_{i+h-1,:}\}$.
    for each filter $j = 1$ till $F_\mathrm{c}$ do
        $[\boldsymbol{O}_\mathrm{c}]_{i,j} \leftarrow \mathrm{ReLu}\big(\bar{\boldsymbol{o}}_i^\mathrm{s}\boldsymbol{h}_j + b_{i,j}\big)$.
    end
end
Other operations:
Obtain $\boldsymbol{o}_\mathrm{f}$ with $\boldsymbol{O}_\mathrm{c}$ in the flatten layer.
Consecutively update the trainable parameters by
    optimizing $\mathcal{L}(\boldsymbol{y})$ with $\boldsymbol{y} \leftarrow \mathrm{sigmoid}(\boldsymbol{W}_\mathrm{D}\boldsymbol{o}_\mathrm{f} + \boldsymbol{b}_\mathrm{D})$.
End
```

```
Algorithm 2: The Hodge AGNN
Input: Flow signal $\boldsymbol{f}$, Incidence matrix $\boldsymbol{B}$
Output: Output $\boldsymbol{O}_\mathrm{s}$ of the Hodge aggregation layer
Hodge AGNN:
Initialization: $\boldsymbol{O}_\mathrm{s} \leftarrow [\ ]$, $\boldsymbol{S} \leftarrow \boldsymbol{B}^\mathrm{T}\boldsymbol{B}/\lambda_\mathrm{max}$
for each shift $i = 1$ till $E_\mathrm{e}$ do
    $\boldsymbol{O}_\mathrm{s} \leftarrow \{\boldsymbol{O}_\mathrm{s}, \boldsymbol{S}^{i-1}\boldsymbol{f}\}$.
end
```

$\boldsymbol{o}_\mathrm{f}$ as the input of the fully connected layer, we can obtain the output of the fully connected layer, namely,

$$\boldsymbol{y} = \sigma(\boldsymbol{W}_\mathrm{D}\boldsymbol{o}_\mathrm{f} + \boldsymbol{b}_\mathrm{D}), \tag{15}$$

where $\boldsymbol{W}_\mathrm{D} \in \mathbb{R}^{E_\mathrm{e} \times E_\mathrm{e}F_\mathrm{c}}$ and $\boldsymbol{b}_\mathrm{D} \in \mathbb{R}^{E_\mathrm{e}}$ respectively denote the trainable matrix and the bias term at the fully connected layer. We utilize the sigmoid function $\mathrm{sigmoid}(x) = 1/(1 + \exp(x))$ as the activation function $\sigma(\cdot)$ in (15). Each entry y_i of the output $\boldsymbol{y} \in \mathbb{R}^{E_\mathrm{e}}$ represents the probability of the corresponding meter i being attacked.

To optimize all the free unknown parameters in the detectors, we consider minimizing the cross-entropy loss function [49]

$$\mathcal{L}(\boldsymbol{y}) = -\frac{1}{E_\mathrm{e}}\sum_{i=1}^{E_\mathrm{e}}\Big(y_{i,\mathrm{o}}\log(y_i) + \big(1 - y_{i,\mathrm{o}}\big)\log(1 - y_i)\Big), \tag{16}$$

with the Adam optimizer [49], where each entry $y_{i,\mathrm{o}}$ of the label $\boldsymbol{y}_\mathrm{o} = [y_{1,\mathrm{o}}, y_{2,\mathrm{o}}, \ldots, y_{E_\mathrm{e},\mathrm{o}}]^\mathrm{T} \in \mathbb{R}^{E_\mathrm{e}}$ indicates whether the corresponding meter is under FDIA. In other words, $y_{i,\mathrm{o}} = 1$ indicates that the meter i is under FDIA; $y_{i,\mathrm{o}} = 0$ indicates that the meter i is FDIA-free. The complete HodgeNet-based detectors are summarized in Algorithm 1. It is noteworthy that the main difference between the Hodge AGNN-based and the Hodge AGAT-based detectors lies in the Hodge aggregation layer. The calculation steps for the proposed Hodge aggregation layer of the different implementations are respectively summarized in Algorithms 2 and 3.

After the free parameters in the detectors have been trained, with the flow signal $\boldsymbol{f}$ as the input, the output of either the proposed Hodge AGNN-based or Hodge AGAT-based detector is given by $\hat{\boldsymbol{y}} \in \mathbb{R}^{E_\mathrm{e}}$, each entry $\hat{y}_i$ of which can be determined by the binary decision

```
Algorithm 3: The Hodge AGAT
Input: Flow signal $\boldsymbol{f}$, Incidence matrix $\boldsymbol{B}$, Number $D$ of
       attention mechanisms
Output: Output $\boldsymbol{O}_\mathrm{s}$ of the Hodge aggregation layer
Initialization: $\boldsymbol{O}_\mathrm{s} \leftarrow [\ ]$
for each attention mechanism $d = 1$ till $D$ do
    Initialization: $\boldsymbol{O}_\mathrm{s}^{(d)} \leftarrow [\ ]$,
    for $i = 1$ till $E_\mathrm{e}$ do
        for $j = 1$ till $E_\mathrm{e}$ do
            $\delta_{i,j} \leftarrow \mathrm{PReLu}\Big(\Big[\big[\boldsymbol{f}\boldsymbol{w}_\mathrm{a}\big]_{i,:} \| \big[\boldsymbol{f}\boldsymbol{w}_\mathrm{a}\big]_{j,:}\Big]\boldsymbol{m}\Big)$.
            $[\boldsymbol{S}]_{i,j} = \mathrm{softmax}\big(\delta_{i,j}\big)$.
        end
        for each shift $i = 1$ till $E_\mathrm{e}$ do
            $\boldsymbol{O}_\mathrm{s}^{(d)} \leftarrow \{\boldsymbol{O}_\mathrm{s}^{(d)}, \boldsymbol{S}^{i-1}\boldsymbol{f}\}$.
        end
    end
    $\boldsymbol{O}_\mathrm{s} \leftarrow \{\boldsymbol{O}_\mathrm{s}, \boldsymbol{O}_\mathrm{s}^{(d)}\}$.
end
```

$$y_i \gtrless \tau, \tag{17}$$

with the threshold $\tau \in (0, 1)$. The hypothesis that false data is injected into the meter i is true if $y_i > \tau$, and $\hat{y}_i$ is accordingly set to 1; otherwise, the alternative hypothesis that meter i is FDIA-free is true, and accordingly $\hat{y}_i = 0$. Without loss of generality, the threshold is set to be 0.5 in the following experiments unless otherwise specified. Obviously, we say that the power system is being attacked when $\|\hat{\boldsymbol{y}}\|_\infty = 1$; we say that the power system is FDIA-free, otherwise. When $\|\hat{\boldsymbol{y}}\|_\infty = 1$, we can locate each attacked meter i, as the corresponding entry $\hat{y}_i$ is equal to 1.

It is noteworthy that in contrast to the other FDIA detectors [19], [20], [27], [28], the Hodge AGNN-based and Hodge AGAT-based detectors could detect and locate the edges or buses with FDIAs simultaneously in the smart grid. As experimentally demonstrated further ahead, making full use of *the spatial correlation* of the edge features via aggregating *the features of neighboring edges in the edge space* in the Hodge aggregation layer would enhance the performance of locational detection of FDIAs.

IV. Simulation Results

We now evaluate the locational detection performance and the computational time of the proposed HodgeNet-based detectors, following the elaboration of the dataset generation and experiment setups. We also validate the robustness of the proposed HodgeNet-based detectors under various circumstances, and the effectiveness of the proposed detectors when meters are only deployed on partial edges of the smart grid.

A. Dataset Generation

We consider herein generating datasets of the classical IEEE 14-bus power system [51] and 39-bus power system by utilizing Pandapower [52] to assess the locational detection performance of FDIA detectors. These two test grids are virtually lossy power systems, the power loss percentages of which are pre-determined with the given topologies and underlying pertinent parameters such as transmission line impedance and transformer losses encapsulated in Pandapower [6], [44], and approximately 4.9% and 0.69%, respectively. Additionally, the power flow measurements on branches and power injection measurements on buses are calculated with the DC optimal power flow analysis [6].

To simulate the realistic operations of power systems, we generate the attack-free data by using the real-world load profiles [29]. Specifically, owing to both the load and generated power values scaled with the scaling parameter ς_i for each bus i in Pandapower, we fit the fluctuation of both the load and generated power values by assigning ς_i with a sample from the normal distribution $\mathcal{N}(1+k[\boldsymbol{s}]_t, \sigma_{\text{s}}^2)$ at each time instance $t \in \{1, \ldots, T\}$. The standardized time series data $\boldsymbol{s} \in \mathbb{R}^T$ is obtained from the ERCOT dataset [53], k represents the intensity of fluctuations of the load and the generated power values, and σ_{s}^2 represents the noise power of the load and the generated power values. We herein set $k = 0.1, \sigma_{\text{s}} = 0.03$, unless stated otherwise. Note that when $k = 0$, the data generation procedure is the same as [17], [20] without fitting the real-world load profile. Then, by implementing the DC optimal power flow analysis in Pandapower, we obtain the corresponding attack-free dataset, including the power flow measurements on each branch and power injections on each bus at each time instance.

We next generate data in the presence of FDIAs, by using the attack-free data generated above. It is noteworthy that real-world attackers would generally choose partial buses as attacked targets, and the detectors generally lack prior knowledge about the attacks. Hence, for brevity, we consider that n randomly selected buses are attacked during each attacked time instance t, and each attacked bus in the attacked bus set $\mathcal{V}_{\text{a}}^{(t)}$ is also randomly selected with equal probability from the buses except for the slack bus [27]. The number n of the attacked buses at each attacked time instance t follows the discrete uniform distribution $\mathcal{U}(n_{\min}, n_{\max})$ [20], with $n_{\min} = 2$ and $n_{\max} = 5$. Each attacked time instance t in the attacked time instance set $\mathcal{T}_{\text{a}}$ is randomly selected with the equal probability from all-time instances. The intensity of attack is measured by the error $[\boldsymbol{c}^{(t)}]_i$, where $i \in \mathcal{V}_{\text{a}}^{(t)}$ and $t \in \mathcal{T}_{\text{a}}$ denote each attacked bus and attacked time instance, respectively. In addition, the intensity of attack is assumed to follow the uniform distribution $\mathcal{U}(c_{\min}, c_{\max})$ with $c_{\min} = 0$ and $c_{\max} = 2$.

In the presence of FDIAs, we obtain the dataset $\mathcal{Z}$, consisting of all the power measurements from each meter in the power grid. Dataset $\mathcal{Z}$ contains $120,000$ time instances, and is divided into the training set comprised of $110,000$ time instances and the testing set comprised of $10,000$ time instances, along with the zero-mean white Gaussian noise with the variance $\sigma_{\text{n}}^2 = 0.01^2$. Moreover, we set the proportion of the attacked time instances in all-time instances as 0.1 for the training set, and set that as 0.5 for the testing set. The dataset generation steps are summarized in Algorithm 4.

Algorithm 4: Dataset Generation

```
Input: IEEE bus system, $\boldsymbol{s}$, $\mathcal{T}_a$, $\mathcal{V}_a^{(t)}$
Output: Dataset $\mathcal{Z}$
Initialization: $k$, $\sigma_{\text{s}}$, $\sigma_{\text{n}}$, $n_{\min}$, $n_{\max}$ $c_{\min}$, $c_{\max}$, $\boldsymbol{c}^{(t)} = \boldsymbol{0}$
  for all instant $t$, the number $T$ of the instances.
for each time instant $t$ till $T$ do
    for each bus $i$ do
        $\varsigma_i \sim \mathcal{N}(1 + k[\boldsymbol{s}]_t, \sigma_{\text{s}}^2)$.
    end
    Through Pandapower, $\boldsymbol{z}^{(t)}$ are obtained by performing
      the DC power flow analysis.
end
for each attacked time instant $t \in \mathcal{T}_a$ do
    for each attacked bus $i \in \mathcal{V}_a^{(t)}$ do
        $[\boldsymbol{c}^{(t)}]_i \sim \mathcal{U}(c_{\min}, c_{\max})$.
    end
    $z^{(t)} \leftarrow z^{(t)} = z_{\text{o}}^{(t)} + \boldsymbol{H}\boldsymbol{c}^{(t)}$.
end
for each time instance $t$ till $T$ and each meter $i$ do
    $[z^{(t)}]_i = [z^{(t)}]_i + n_z$, $n_z \sim \mathcal{N}(0, \sigma_{\text{n}}^2)$,
    $\mathcal{Z} \leftarrow \{\mathcal{Z}, [z^{(t)}]_i\}$.
end
```

B. Implementation Issues and Performance Metrics

All the implementations are conducted in Python 3.7 using Pandapower [52], pytorch [54], and sklearn [55] on Intel Core i7-11700 CPU with NVIDIA GeForce RTX 3080 Ti GPU. We compare our proposed methods with their benchmark competitors of the DT [15], [56], Gaussian Naive Bayes (GNB) [57], SVM [15], [18], [56], [58], [59], Multi-Label KNN [18], [59], [60], MLP [19] and CNN [20].

To assess the locational detection performance of the aforementioned FDIA detectors, we use Recall $=$ TP/(TP $+$ FN) and Precision $=$ TP/(TP $+$ FP) as the performance metrics. Herein, True Positive (TP), False Positive (FP), and False Negative (FN) respectively denote the counts of the samples that the attacked bus is correctly classified as attacked, the normal bus is incorrectly classified as attacked, and the attacked bus is incorrectly classified as normal. We then calculate the $F_1 = (2\text{Recall} \times \text{Precision})/(\text{Recall} + \text{Precision})$ score [61], which is the harmonic mean of the Precision and Recall of the detector. Furthermore, to evaluate the edge-wise accuracy of the locational detection for FDIAs, we utilize the Locational Detection Rate, LDR $=$ (TP $+$ TN)/(TP $+$ FP $+$ FN $+$ TN) [20], where True Negative (TN) denotes the count of the samples that the normal buses are correctly classified as normal for all time instances. Additionally, to evaluate the detection performance of the aforementioned FDIA detectors, we also utilize the Presence Detection Rate (PDR), which is

TABLE I
LOCATIONAL DETECTION RESULTS FOR THE IEEE 14-BUS TEST GRID

Model	Precision(%)	Recall(%)	F_1(%)	PDR(%)	LDR(%)
DT	87.75	70.57	78.23	51.76	90.75
GNB	92.91	93.61	93.26	77.79	96.81
SVM	95.78	82.53	88.66	71.93	95.03
KNN	94.11	81.88	87.57	67.31	94.52
MLP	98.38	96.16	97.26	81.53	98.73
CNN	98.86	98.06	98.46	87.70	99.28
Hodge AGNN	99.02	97.97	98.49	89.23	99.29
Hodge AGAT	**99.45**	**98.55**	**99.00**	**93.54**	**99.53**

TABLE II
LOCATIONAL DETECTION RESULTS IN THE IEEE 39-BUS TEST GRID

Model	Precision(%)	Recall(%)	F_1(%)	PDR(%)	LDR(%)
DT	94.71	46.88	62.72	51.81	94.74
GNB	57.67	60.09	58.86	22.98	92.07
SVM	84.59	41.62	55.79	53.60	93.78
KNN	89.75	54.09	67.50	52.95	95.09
MLP	96.70	90.50	93.50	71.17	98.81
CNN	96.78	94.85	95.80	76.28	99.22
Hodge AGNN	97.80	94.06	95.89	77.95	99.24
Hodge AGAT	**98.15**	**95.07**	**96.59**	**81.28**	**99.37**

the probability that the power system is correctly classified as attacked or not. Those performance metrics for each experiment hereinafter are obtained by averaging 5 independent trials for each model.

Based on the random search strategy, the hyperparameters, such as the number of layers, the number of units of the hidden feature, and the number of independent attention mechanisms, are selected by utilizing the F_1 score to evaluate locational detection performance.

C. Locational Detection Performance

We investigate the locational detection performance of both the Hodge AGNN-based and Hodge AGAT-based detectors by comparing with their competitors in the IEEE 14-bus and 39-bus power systems. The locational detection results (Precision, Recall, F_1, PDR and LDR) of those detectors are shown in the Tables I and II.

As illustrated in Table I, the Neural Network (NN)-based detectors (the MLP, CNN, Hodge AGNN and Hodge AGAT) are observed to outperform the detectors based on the conventional machine learning such as the DT, GNB, SVM, and KNN. Specially, compared with the other NN-based detectors, the MLP-based detector does not perform quite well as it tends to overfit the training data and fail to generalize possibly due to its fully connected relationship between its units. Benefiting from the use of the underlying topologies of the smart grid, both the Hodge AGNN-based and Hodge AGAT-based detectors are observed to outperform their competitors. Additionally, compared with the Hodge AGNN-based detector, we can observe in Table I that the Hodge AGAT-based detector enhances the locational detection performance, since the Hodge AGAT-based detector exploits the graph attention mechanism to adapt the weights of the Hodge Laplacian. Specifically, compared with the metrics of Precision, Recall, F_1, PDR and LDR of the Hodge AGNN-based detector, the corresponding metrics of the Hodge AGAT-based detector exceed by 0.43%, 0.58%, 0.51%, 4.31% and 0.24%, respectively.

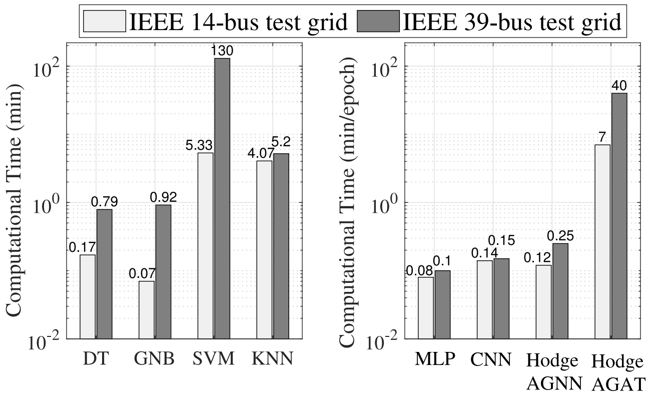


Fig. 3. The computational time of different detectors.

We further evaluate the locational detection performance of the proposed HodgeNet-based detector for the IEEE 39-bus test grid. As demonstrated in Table II, the locational detection performance of the conventional machine learning-based detection methods (DT, GNB, SVM, KNN) and the NN-based detection methods (MLP, CNN, Hodge AGNN, Hodge AGAT) all deteriorates for the IEEE 39-bus test grid. Whereas the NN-based detectors are observed to be more robust to the different scales of the power systems. Notice that leveraging the underlying topologies of the smart grids, both the proposed Hodge AGNN-based and Hodge AGAT-based detectors are observed to outperform the competing models. Additionally, as illustrated in Table II, the Hodge AGAT-based detector is observed to outperform the Hodge AGNN-based detector.

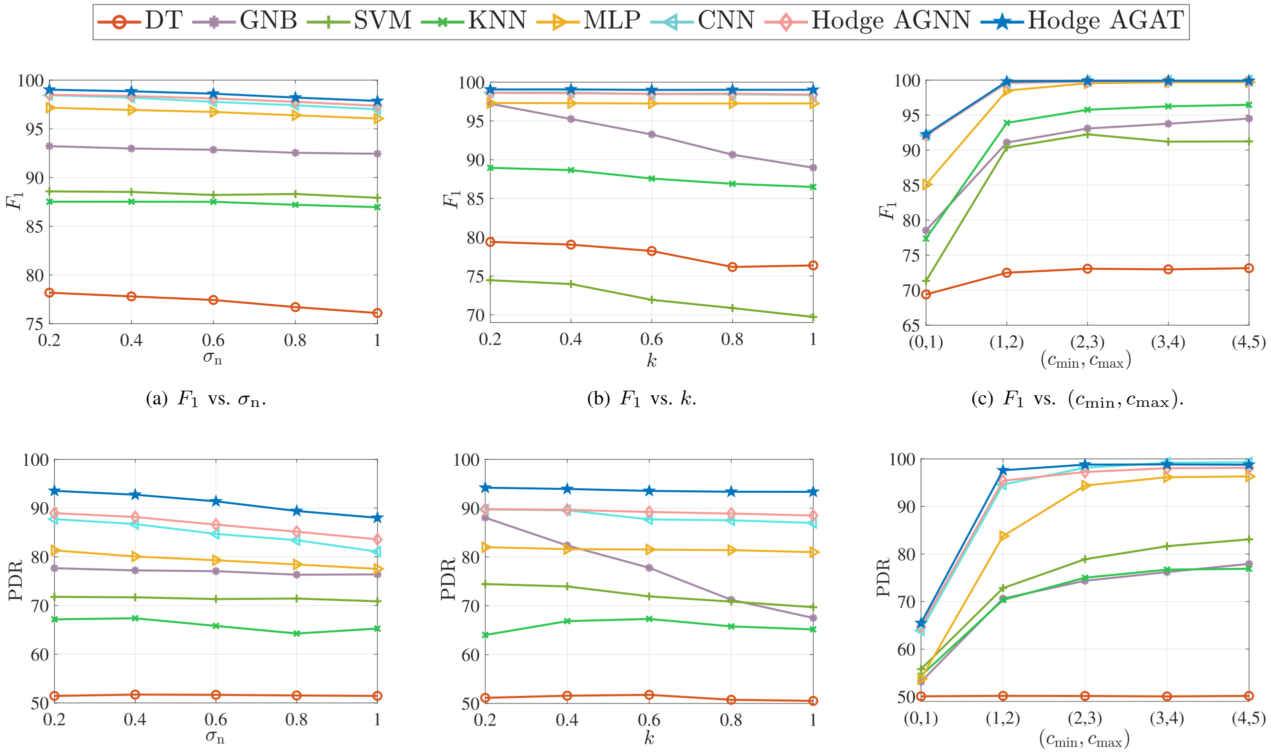
D. Computational Time

We compare the computational time of different detectors for the IEEE 14-bus and 39-bus test grids. We consider respectively deploying 34 and 85 meters for the IEEE 14-bus and 39-bus test grids. Regarding the IEEE 14-bus test grid, it is observed in Fig. 3 that both the SVM-based and KNN-based FDIA detectors would spend longer time than the DT-based and GNB-based detectors. According to our experiments, the NN-based methods could usually achieve algorithmic convergence within about 60 epochs. The proposed HodgeNet-based detectors are observed to obtain superior detection performance at the cost of computational time. Whereas the computational efficiency of the proposed Hodge AGNN-based detector is superior to that of the proposed Hodge AGAT-based detector.

We have the similar computational time results for the IEEE 39-bus test grid. Moreover, we can also observe the increase of the computational time of all the detectors for the IEEE 39-bus test grid, compared with that for the IEEE 14-bus test grid. It is observed that the computational time of the SVM-based and the proposed Hodge AGAT-based detectors is more closely pertinent to the scale of the test grids.

E. Robustness Validation

We respectively evaluate the effects of the additive noise during data acquisition, the fluctuation intensities of both the



(a) F_1 vs. σ_n.

(b) F_1 vs. k.

(c) F_1 vs. $(c_{\min}, c_{\max})$.

(d) PDR vs. σ_n.

(e) PDR vs. k.

(f) PDR vs. $(c_{\min}, c_{\max})$.

Fig. 4. The robustness validation of the proposed HodgeNet-based detectors and their competitors.

load and the power generation value, as well as the intensities of the FDIAs on the performance of both the proposed Hodge AGNN-based and Hodge AGAT-based detectors.

We first evaluate the effects of the additive noise on the performance of the FDIA detectors by varying the standard deviation σ_n of the additive noise. The performance (F_1 and PDR) of the FDIA detectors for different noise powers is shown in Figs. 4(a) and 4(d). It could be observed that the locational performance of all the detectors deteriorates with the increase of the noise power, as the noise-free data is more likely drowned in the noises, resulting in that normal data and compromised data are more difficult to distinguish. Whereas the locational performance of both the HodgeNet-based detectors is still superior to that of their competitors, especially in terms of the PDR. Furthermore, the Hodge AGAT-based detector exhibits the superior locational performance of locating both attacked meters and attacked system, compared to the Hodge AGNN-based detector, as shown in Figs. 4(a) and 4(d).

Next, by varying the parameter k of the dataset, we evaluate the impacts of the fluctuation intensities of the load and generated power values on buses. As illustrated in Figs. 4(b) and 4(e), the proposed HodgeNet-based detectors and the other deep learning-based detectors are less sensitive against the change of the fluctuation intensities, whereas the performance of detectors based on the traditional machine learning (the DT, GNB, SVM and KNN) would deteriorate with the increase of k as shown in Fig. 4(b). Notice that the locational performance of the HodgeNet-based detectors is observed to be superior to that of their competitors both in Fig. 4(b) and in Fig. 4(e), and the Hodge AGAT-based detector is observed to outperform the Hodge AGNN-based detector.

Finally, we evaluate the effects of the intensities of the FDIAs on the performance of the FDIA detectors for different ranges of $(c_{\min}, c_{\max})$. Particularly, we consider that the attack error $[\boldsymbol{c}^{(t)}]_i$ on each attacked bus i is random, and can be either negative or positive. As the increase of the intensities of the FDIAs results in the difficulty reduction of the locational detection for FDIAs, the locational detection performance of the HodgeNet-based detectors is increased with the increasing intensities of the FDIAs, as illustrated in Figs. 4(c) and 4(f). Specially, when the attack voltage phase angle reaches around 2 degree, the F_1's of the proposed FDIA detectors approach 100%. Notice that the HodgeNet-based detectors, especially the Hodge AGAT-based detector, are observed to achieve superior locational detection performance compared to their competitors, even under a slight attack.

F. Partial Observation

The previous experiments exploit the power measurements on both all the branches and buses in the smart grid ($M = E_e = 34$). We now consider evaluating the locational detection performance of the proposed FDIA detectors when data of only partial branches or buses can be available in real-world applications, due to the limited meter resources or the loss of the data on some branches or buses, i.e., we could only observe M ($M < E_e$) edges in the reconstruction graph.

We observe $M = 28$ and $M = 22$ edges randomly selected with equal probability from $E_e = 34$ edges of the reconstruction graph, and the selected edges are dubbed the observed edges. To obtain the observed edges, we define the binary row-selection matrix $\boldsymbol{P} \in \{0, 1\}^{M \times E_e}$, where $\boldsymbol{P}$ satisfies $\boldsymbol{P}\mathbf{1} = \mathbf{1}$ and $[\boldsymbol{P}]_{i,j} = 1$ if jth edge is observed. The input signal

TABLE III
LOCATION DETECTION RESULTS OF PARTIAL OBSERVATIONS

Model	M	Precision(%)	Recall(%)	F_1(%)	PDR(%)	LDR(%)
DT	28	86.69	65.05	74.33	51.39	89.41
	22	86.99	66.59	75.44	50.85	89.78
GNB	28	92.91	90.41	91.64	75.79	96.12
	22	92.54	90.48	91.50	73.16	96.04
SVM	28	95.60	81.98	88.27	71.63	94.87
	22	95.39	80.89	87.55	68.84	94.58
KNN	28	93.91	81.81	87.44	67.26	94.47
	22	91.41	82.75	86.86	61.57	94.11
MLP	28	98.32	95.34	96.81	80.31	98.52
	22	97.96	95.45	96.69	78.86	98.46
CNN	28	98.60	97.41	98.00	85.40	99.07
	22	98.10	97.02	97.55	82.60	98.86
Hodge AGNN	28	98.76	97.30	98.03	86.73	99.08
	22	98.45	97.51	97.98	86.24	99.06
Hodge AGAT	28	**99.28**	**98.39**	**98.83**	**92.72**	**99.45**
	22	**99.25**	**98.31**	**98.78**	**92.35**	**99.43**

of the HodgeNet-based detectors can be given by $\boldsymbol{f} \in \mathbb{R}^{E_\mathrm{e}}$, where $[\boldsymbol{f}]_j \neq 0$, $j \in \mathcal{E}_\mathrm{e}^{(M)}$, where $\mathcal{E}_\mathrm{e}^{(M)} \subset \mathcal{E}_\mathrm{e}$ is the observed edge set with its cardinality $|\mathcal{E}_\mathrm{e}^{(M)}| = M$; and $[\boldsymbol{f}]_j = 0$, otherwise. In light of (9), the output of the Hodge aggregation layer can be rewritten as

$$\boldsymbol{O}_\mathrm{s}^{(M)} = \boldsymbol{P}\Big[\boldsymbol{f}, \boldsymbol{L}_1\boldsymbol{f}, \boldsymbol{L}_1^2\boldsymbol{f}, \ldots, \boldsymbol{L}_1^{E_\mathrm{e}-1}\boldsymbol{f}\Big]. \tag{18}$$

When the data of only partial branches or buses can be observed, the locational detection performance of all the FDIA detectors is shown in Table III.

As shown in Table III, we can observe that the locational detection performance of all the detectors slightly deteriorates with either $M = 22$ or $M = 28$ edges of the reconstruction graph. As the CNN-based detector captures the inconsistencies owing to FDIAs by utilizing the correlation of the adjacent measurements, the CNN-based FDIA detector exhibits superior locational detection performance, compared to the other benchmark competitors (the DT, GNB, SVM, KNN and MLP). Additionally, the proposed HodgeNet-based detectors have more ascendancy over the CNN-based detector, as both the proposed detectors incorporate the underlying graph topology of the power grid, and could reveal the spatial proximity among the features on neighboring meters rather than the adjacent measurements. Specifically, as illustrated in Table III, the F_1's of the Hodge AGNN-based and Hodge AGAT-based detectors are superior to that of the CNN-based detector by 0.03% and 0.83%. Likewise, the PDRs of the proposed detectors are superior to that of the CNN-based detector by 1.33% and 7.32%, respectively.

V. CONCLUSION

In this paper, we consider utilizing both the power flows on branches and power injections on buses to detect and locate FDIAs on smart grids, and then correspondingly propose a distinctive graph representation of power systems via adding an imaginary node and edges. Based on the Hodge theory, we develop a Hodge AGNN-based FDIA detector in the edge space by utilizing the inherent graph structure of smart grids. We further incorporate the graph attention mechanism into the aforementioned FDIA detector, and propose a Hodge AGAT-based FDIA detector. The superior locational detection performance of the proposed detectors is validated through illustrative simulations for the IEEE 14-bus and 39-bus test grids, at the expense of computational time. Moreover, the proposed detectors are experimentally validated to be robust to additive noises during data acquisition, fluctuation intensities of both the load and power generation values, as well as the intensities of FDIAs. The feasibility of the proposed detectors for locational detection of FDIAs on smart grids with irregular topologies is also experimentally demonstrated in the scenarios when only partial edges can be observed.

REFERENCES

[1] H. M. Khalid, S. M. Muyeen, and J. C.-H. Peng, "Cyber-attacks in a looped energy-water nexus: An inoculated sub-observer-based approach," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2054–2065, Jun. 2020.

[2] U. Inayat, M. F. Zia, S. Mahmood, H. M. Khalid, and M. Benbouzid, "Learning-based methods for cyber attacks detection in IoT systems: A survey on methods, analysis, and future prospects," *Electronics*, vol. 11, no. 9, p. 1502, May 2022.

[3] Y. Lu and L. D. Xu, "Internet of Things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2103–2115, Apr. 2019.

[4] H. M. Khalid et al., "WAMS operations in power grids: A track fusion-based mixture density estimation-driven grid resilient approach toward cyberattacks," *IEEE Syst. J.*, vol. 17, no. 3, pp. 3950–3961, Sep. 2023.

[5] M. Thomas and J. McDonald, *Power System SCADA and Smart Grids*. Boca Raton, FL, USA: CRC Press, 2017.

[6] A. Abur and A. G. Expósito, *Power System State Estimation: Theory and Implementation*. New York, NY, USA: Marcel Dekker, 2004.

[7] H. M. Khalid, F. Flitti, M. S. Mahmoud, M. M. Hamdan, S. M. Muyeen, and Z. Y. Dong, "Wide area monitoring system operations in modern power grids: A median regression function-based state estimation approach towards cyber attacks," *Sustain. Energy, Grids Netw.*, vol. 34, Jun. 2023, Art. no. 101009.

[8] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inform. Syst. Secur.*, vol. 14, no. 1, pp. 1–33, May 2011.

[9] 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 Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[10] M. M. N. Aboelwafa, K. G. Seddik, M. H. Eldefrawy, Y. Gadallah, and M. Gidlund, "A machine-learning-based technique for false data injection attacks detection in industrial IoT," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8462–8471, Sep. 2020.

[11] N. N. Tran, H. R. Pota, Q. N. Tran, and J. Hu, "Designing constraint-based false data-injection attacks against the unbalanced distribution smart grids," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 9422–9435, Jun. 2021.

[12] A. E. L. Rivas and T. Abrão, "Faults in smart grid systems: Monitoring, detection and classification," *Electric Power Syst. Res.*, vol. 189, Dec. 2020, Art. no. 106602.

[13] X. Zeng, K. K. Li, W. L. Chan, S. Su, and Y. Wang, "Ground-fault feeder detection with fault-current and fault-resistance measurement in mine power systems," *IEEE Trans. Ind. Appl.*, vol. 44, no. 2, pp. 424–429, Mar. 2008.

[14] S. Kiranyaz, A. Gastli, L. Ben-Brahim, N. Al-Emadi, and M. Gabbouj, "Real-time fault detection and identification for MMC using 1-D convolutional neural networks," *IEEE Trans. Ind. Electron.*, vol. 66, no. 11, pp. 8760–8771, Nov. 2019.

[15] A. Jindal, A. Dua, K. Kaur, M. Singh, N. Kumar, and S. Mishra, "Decision tree and SVM-based data analytics for theft detection in smart grid," *IEEE Trans. Ind. Informat.*, vol. 12, no. 3, pp. 1005–1016, Jun. 2016.

[16] P. K. Jena, S. Ghosh, E. Koley, and M. Manohar, "An ensemble classifier based scheme for detection of false data attacks aiming at disruption of electricity market operation," *J. Netw. Syst. Manage.*, vol. 29, no. 4, p. 43, Oct. 2021.

[17] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1644–1652, Sep. 2017.

[18] D. Wang, X. Wang, and Y. Zhang, and L. Jin, "Detection of power grid disturbances and cyber-attacks based on machine learning," *J. Inform. Secur. Appl.*, vol. 46, pp. 42–52, Jun. 2019.

[19] A. Tabakhpour and M. M. A. Abdelaziz, "Neural network model for false data detection in power system state estimation," in *Proc. IEEE Can. Conf. Elect. Comput. Eng. (CCECE)*, 2019, pp. 1–5.

[20] S. Wang, S. Bi, and Y.-J. A. Zhang, "Locational detection of the false data injection attack in a smart grid: A multilabel classification approach," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8218–8227, Sep. 2020.

[21] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2218–2234, May 2020.

[22] Y. Zhang, J. Wang, and B. Chen, "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 623–634, Jan. 2021.

[23] Y. Li, X. Wei, Y. Li, Z. Dong, and M. Shahidehpour, "Detection of false data injection attacks in smart grid: A secure federated deep learning approach," *IEEE Trans. Smart Grid*, vol. 13, no. 6, pp. 4862–4872, Nov. 2022.

[24] Q. Yang, D. An, R. Min, W. Yu, X. Yang, and W. Zhao, "On optimal PMU placement-based defense against data integrity attacks in smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 7, pp. 1735–1750, Jul. 2017.

[25] W. Lei, Z. Pang, H. Wen, W. Hou, and W. Han, "FDI attack detection at the edge of smart grids based on classification of predicted residuals," *IEEE Trans. Ind. Informat.*, vol. 18, no. 12, pp. 9302–9311, Dec. 2022.

[26] R. Ramakrishna and A. Scaglione, "Grid-graph signal processing (grid-GSP): A graph signal processing framework for the power grid," *IEEE Trans. Signal Process.*, vol. 69, pp. 2725–2739, Apr. 2021.

[27] E. Drayer and T. Routtenberg, "Detection of false data injection attacks in power systems with graph fourier transform," in *Proc. IEEE Glob. Conf. Signal Inform. Process. (GlobalSIP)*, 2018, pp. 890–894.

[28] E. Drayer and T. Routtenberg, "Detection of false data injection attacks in smart grids based on graph signal processing," *IEEE Syst. J.*, vol. 14, no. 2, pp. 1886–1896, Jun. 2020.

[29] O. Boyaci et al., "Graph neural networks based detection of stealth false data injection attacks in smart grids," *IEEE Syst. J.*, vol. 16, no. 2, pp. 2946–2957, Jun. 2022.

[30] R. Ramakrishna and A. Scaglione, "Detection of false data injection attack using graph signal processing for the power grid," in *Proc. IEEE Glob. Conf. Signal Inform. Process. (GlobalSIP)*, 2019, pp. 1–5.

[31] R. Ramakrishna and A. Scaglione, "On modeling voltage phasor measurements as graph signals," in *Proc. IEEE Data Sci. Workshop (DSW)*, 2019, pp. 275–279.

[32] W. Xia, D. He, and J. Chen, "On the PMU placement optimization for the detection of false data injection attacks," *IEEE Syst. J.*, vol. 17, no. 3, pp. 3794–3797, Sep. 2023.

[33] T. N. Kipf and M. Welling, "Semi-supervised classification with graph convolutional networks," 2017, *arXiv:1609.02907*.

[34] F. Gama, A. G. Marques, G. Leus, and A. Ribeiro, "Convolutional neural network architectures for signals supported on graphs," *IEEE Trans. Signal Process.*, vol. 67, no. 4, pp. 1034–1049, Feb. 2019.

[35] W. Xia, D. He, and L. Yu, "Locational detection of false data injection attacks in smart grids: A graph convolutional attention network approach," *IEEE Internet Things J.*, vol. 11, no. 6, pp. 9324–9337, Mar. 2024.

[36] M. T. Schaub and S. Segarra, "Flow smoothing and denoising: Graph signal processing in the edge-space," in *Proc. IEEE Glob. Conf. Signal Inform. Process. (GlobalSIP)*, 2018, pp. 735–739.

[37] M. T. Schaub, A. R. Benson, P. Horn, G. Lippner, and A. Jadbabaie, "Random walks on Simplicial complexes and the Normalized Hodge 1-Laplacian," *SIAM Rev.*, vol. 62, no. 2, pp. 353–391, Jan. 2020.

[38] T. M. Roddenberry and S. Segarra, "HodgeNet: Graph neural networks for edge data," in *Proc. 53rd Asilomar Conf. Signals, Syst., Comput. (ACSSC)*, 2019, pp. 220–224.

[39] M. Yang, E. Isufi, M. T. Schaub, and G. Leus, "Finite impulse response filters for simplicial complexes," in *Proc. 29th Eur. Signal Process. Conf. (EUSIPCO)*, 2021, pp. 2005–2009.

[40] L.-H. Lim, "Hodge Laplacians on graphs," *SIAM Rev.*, vol. 62, no. 3, pp. 685–715, Jan. 2020.

[41] M. T. Schaub, J.-B. Seby, F. Frantzen, T. M. Roddenberry, Y. Zhu, and S. Segarra, "Signal processing on simplicial complexes," 2022, *arXiv: 2106.07471*.

[42] S. Barbarossa and S. Sardellitti, "Topological signal processing over simplicial complexes," *IEEE Trans. Signal Process.*, vol. 68, pp. 2992–3007, Mar. 2020.

[43] M. Yang, E. Isufi, M. T. Schaub, and G. Leus, "Simplicial convolutional filters," *IEEE Trans. Signal Process.*, vol. 70, pp. 4633–4648, Sep. 2022.

[44] A. J. Wood, B. F. Wollenberg, and G. B. Sheblé, *Power Generation, Operation and Control*. New York, NY, USA: Wiley, 2014.

[45] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–621, Mar. 2014.

[46] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[47] P. Veličković, G. Cucurull, A. Casanova, A. Romero, P. Liò, and Y. Bengio, "Graph attention networks," 2018, *arXiv:1710.10903*.

[48] C. W. J. Goh, C. Bodnar, and P. Liò, "Simplicial attention networks," 2022, *arXiv:2204.09455*.

[49] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.

[50] Y. Kim, "Convolutional neural networks for sentence classification," 2014, *arXiv:1408.5882*.

[51] R. Christie. "Power systems test case archive." 1993. [Online]. Available: http://labs.ece.uw.edu/pstca/pf14/pg tca14bus.htm

[52] L. Thurner et al., "Pandapower—An open-source python tool for convenient modeling, analysis, and optimization of electric power systems," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6510–6521, Nov. 2018.

[53] (Electr. Reliab. Counc. Texas Corp., Austin, TX, USA). *Backcasted (Actual) Load Profiles—Historical*. (2020). [Online]. Available: http://www.ercot.com/mktinfo/loadprofile/alp/

[54] A. Paszke et al., "PyTorch: An imperative style, high-performance deep learning library," in *Proc. 33rd Adv. Neural Inform. Process. Syst.*, 2019, pp. 8024–8035.

[55] F. Pedregosa et al., "Scikit-learn: Machine learning in python," *J. Mach. Learn. Res.*, vol. 12, pp. 2825–2830, Nov. 2011.

[56] K. Vimalkumar and N. Radhika, "A big data framework for intrusion detection in smart grids using apache spark," in *Proc. Int. Conf. Adv. Comput., Commun. Inform. (ICACCI)*, 2017, pp. 198–204.

[57] S. Xu, "Bayesian naïve Bayes classifiers to text classification," *J. Inform. Sci.*, vol. 44, no. 1, pp. 48–59, Feb. 2018.

[58] D. A. Pisner and D. M. Schnyer, "Chapter 6—Support vector machine," in *Machine Learning*. New York, NY, USA: Academic, 2020, pp. 101–121.

[59] J. Yan, B. Tang, and H. He, "Detection of false data attacks in smart grid with supervised learning," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, 2016, pp. 1395–1402.

[60] M.-L. Zhang and Z.-H. Zhou, "ML-KNN: A lazy learning approach to multi-label learning," *Pattern Recognit. Lett.*, vol. 40, no. 7, pp. 2038–2048, Jul. 2007.

[61] T. Fawcett, "An introduction to ROC analysis," *Pattern Recognit. Lett.*, vol. 27, no. 8, pp. 861–874, Jun. 2006.

Wei Xia received the B.S. degree in communication engineering and the M.S. and Ph.D. degrees in signal and information processing from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2002, 2005, and 2008, respectively, where he was with the School of Electronic Engineering from 2009 to 2017. From March 2015 to March 2016, he had been on a 12-month sabbatical leave as a Visiting Scholar with the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ, USA. Since 2018, he has been with the School of Information and Communication Engineering, UESTC, where he is an Associate Professor. Since August 2023, he has been with the School of Computer Science and Technology and the School of Cyberspace Security, Xinjiang University, Ürümqi, China.. His general research interests include statistical signal processing, adaptive signal processing, radar signal processing, and advanced implementation techniques of signal processing algorithms.

Yan Li received the B.E. degree from Dalian Maritime University, Dalian, China, in 2022. He is currently pursuing the M.S. degree with the School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu, China. His current research interests include smart grid security and point cloud registration.

Lisha Yu received the B.S. degree from the Harbin Institute of Technology University, Weihai, China, in 2020 and the M.S. degree from the School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu, China, in 2023. She is currently with the Department of Protocol Product Center, China Star Network Application Company Ltd., Chongqing, China. Her research interests include smart grid security, distributed graph signal processing, and beamforming technology.

Deming He received the B.E. degree from Hohai University, Nanjing, China, in 2021. He is currently pursuing the M.S. degree with the School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu, China. His current research interests include smart grid security and emitter localization technology.