International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

IJIEMR Transactions, online available on 5th Jan 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 01

DOI: 10.48047/IJIEMR/V12/ISSUE 01/04

Title **A Novel Framework for Cyberattack Detection Model for Distribution Systems Based on Spatiotemporal Patterns and Machine Learning Techniques**

Volume 12, ISSUE 01, Pages: 43-51

Paper Authors

Kesoju Sairam, Macha Pooja, P. Shanmukha Kumar

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

A Novel Framework for Cyberattack Detection Model for Distribution Systems Based on Spatiotemporal Patterns and Machine Learning Techniques

Kesoju Sairam[*], Macha Pooja[1], P. Shanmukha Kumar[2]
[*]Assistant Professor, CSE Department, Nalla Narsimha Reddy Group of Institutions, Hyderabad. Email: saikumar581@gmail.com
[1]Assistant Professor, CSE Department, Nalla Narsimha Reddy Group of Institutions, Hyderabad. Email: poojasathish2960@gmail.com
[2]Assistant Professor, CSE Department, Nalla Narsimha Reddy Group of Institutions, Hyderabad. Email: shanmukha6210@gmail.com

Abstract

Due to increase of distributed computing environments the internet traffic increased abnormally and which causes security aspects of from unauthorized attackers. This motivates us to develop a machine learning based cyberattack detection model for distributed environments. The main investment of our work is spatiotemporal patterns for fixing cyberattacks. These patterns are identified by the graph Laplacian based measurements of a wide system. The machine learning techniques helped us to train these spatial and temporal patterns will give an alert when cyberattack occurred. We used a Bayes Classifier for this purpose along with IEEE 13 and 123 node test feeders. We also adapted LSTM methodology to improve our results it proved that our results better than the existed comparatively with an accuracy of 94.3%.

Keywords: Machine learning, LSTM, BC, spatiotemporal patterns, autocoders, distribution systems, graph Laplacian and cyberattack.

1. Introduction

The rapid changes in distributed energy resources changed the pace of technological world completely, designing and operating process too such as micro grids, power grids etc. Sensor technology in support of the existing technologies leads to a powerful working mechanism. The supervisory Control and Data Acquisition (SCADA) techniques improved the smart readings and increased accuracy. Due to increase of sensors in micro-PMUs [3] the development and deployment of the AMI (Advanced Metering Infrastructure) in grid and distribution systems controls the cyber-attacks and distribution management. Data analytics do our job easy in calculations to give proper decision making and exchange of information to handle cyber attack with the help of DMS (Distribution System Management) [1].

We studied the existed works related to it, still facing problems in handling cyberattacks efficiently. Hence we felt that to develop a new approach to handle cyberattacks detection mechanism in distributed environment. Our model support and enables for proper DMS functioning, reliable accuracy, efficient energy delivery and to detect attacks in time for further process dynamically. For this purpose, we used classification techniques such as Naïve Bayes Classifier which uses tribalistic approaches on train and error base [5].

By using BC (Basian Classifier) [7] we captured spatiotemporal attributes continuously with flexible BCs to find the pattern to detect occurring of cyber-attack prone. Under normal conditions the spatiotemporal patterns ignore the cyberattack and unable to handle. Which leads to how to handle cyberattack detection in DMS by using spatiotemporal patterns quantitively with normal conditions and cyberattack prone conditions and can increase the accuracy of cyberattack detection model by using Bayes Classifiers comfortably. We focussed on integration of patterns into BCs for handling attacks. These patterns are analysed by using [2] GGL (Generalized Graph Laplacian) with the given measurements. BCs trains input variables where as cyberattack templates are considered as output variables. We conducted a series test in online by using these patterns and are captured by GGL to work BC work properly and the output results shows cyberattack detection. Finally, this approach will be demonstrated by IEEE-13 and 123.

The rest of the work is organized as, section II explains about BC for detection along with patterns and graph Laplacian mechanism with few case studies, section III covers DMS and result analysis, section IV explains about GGL, section V gives BC and results analysis and finally section VI concludes the work.

CYBER ATTACK DETECTION MODEL

The detection mechanism is developed by using a flexible machine learning technique. Fig 1 shows the full architecture of development of cyberattack detection model. Our proposed model uses

- GGL (Generalized Graph Laplacian) approach it is an unsupervised ML method, it is used to train the patterns measurements.
- Bayes Classifier uses for training of spatiotemporal patterns which are characterized by GGL matrix.
- The performance was evaluated by using true positive rate and confusion matrix table then performance of detection model.

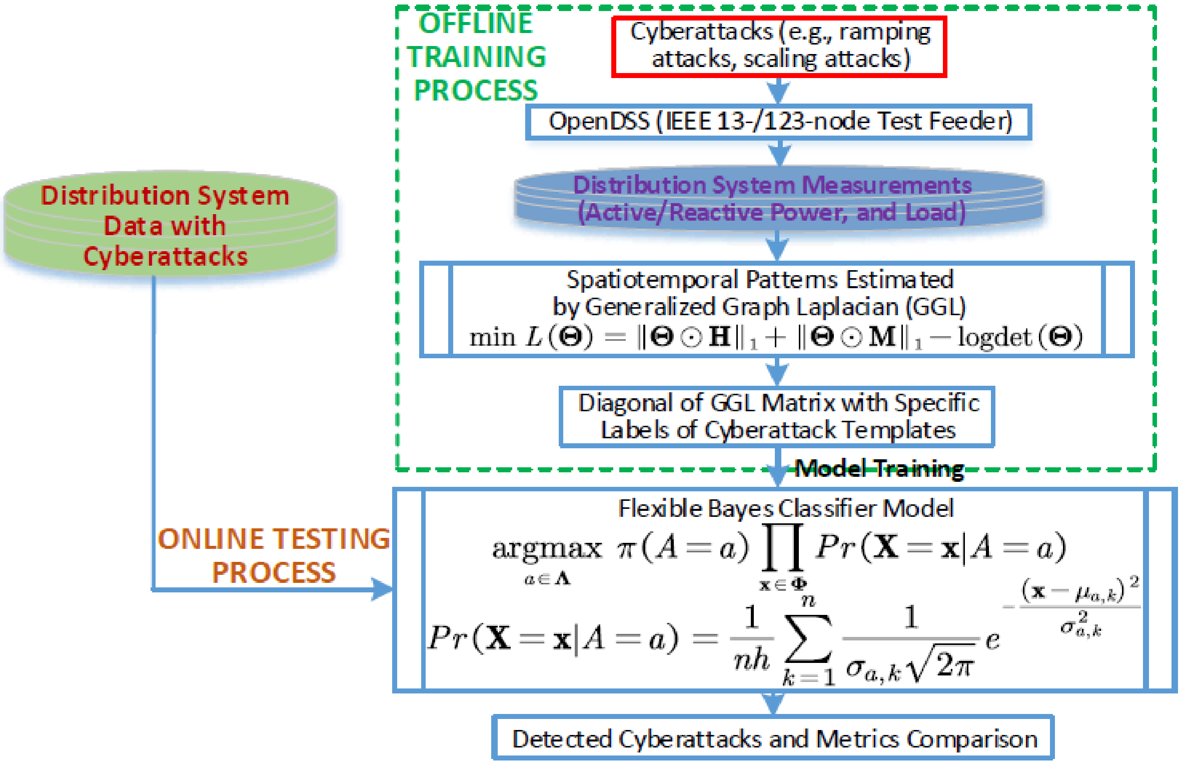

OFFLINE TRAINING PROCESS
Cyberattacks (e.g., ramping attacks, scaling attacks)
OpenDSS (IEEE 13-/123-node Test Feeder)
Distribution System Measurements (Active/Reactive Power, and Load)
Spatiotemporal Patterns Estimated by Generalized Graph Laplacian (GGL)
$\min L(\mathbf{\Theta}) = \|\mathbf{\Theta} \odot \mathbf{H}\|_1 + \|\mathbf{\Theta} \odot \mathbf{M}\|_1 - \operatorname{logdet}(\mathbf{\Theta})$
Diagonal of GGL Matrix with Specific Labels of Cyberattack Templates
Model Training
Distribution System Data with Cyberattacks
ONLINE TESTING PROCESS
Flexible Bayes Classifier Model
$\underset{a \in \mathbf{A}}{\operatorname{argmax}}\ \pi(A=a) \prod_{\mathbf{x} \in \mathbf{\Phi}} Pr(\mathbf{X}=\mathbf{x}|A=a)$
$Pr(\mathbf{X}=\mathbf{x}|A=a) = \frac{1}{nh} \sum_{k=1}^{n} \frac{1}{\sigma_{a,k}\sqrt{2\pi}} e^{-\frac{(\mathbf{x}-\mu_{a,k})^2}{\sigma_{a,k}^2}}$
Detected Cyberattacks and Metrics Comparison

Fig. 1. Architecture of cyberattack detection model.

Generalized Graph Laplacian

It is an unsupervised ML method used to represent graph learning quantitively for spatiotemporal patterns. The edges can be maintained by GGL based on positive weights and negative weights provided in addition. GGL matrix is estimated by Lagrangian optimization technique can be used as.

$$\min L(\Theta) = \|\Theta \odot \mathbf{H}\|_1 + \|\Theta \odot \mathbf{M}\|_1 - \operatorname{logdet}(\Theta) \quad (1$$

$$\mathcal{L}(\mathbf{A}) = \left\{ \Theta \in \mathcal{L} \;\middle|\; \begin{array}{l} (\Theta)_{ij} \leq 0 \text{ if } (\mathbf{A})_{ij} = 1 \\ (\Theta)_{ij} = 0 \text{ if } (\mathbf{A})_{ij} = 0 \end{array} \right\}_{\forall i,j\; i \neq j} \quad (2$$

Where H is the regularization matrix and H = (I - II). I is an specific matrix. II is an all-ones matrix. is the regularization parameter. II is the projected GGL matrix. L is the goal set of graph Laplacians. A is the similarity matrix. © manner the element-clever multiplication of matrices. ||.||1 manner the sum of absolute values of all elements (`1-norm). logdet (.) manner the herbal logarithm of a determinant. M is the Lagrange multiplier matrix.

Bayes Classifiers

By using spatiotemporal patterns as inputs, traditional naive BCs are generally handled with the useful resource of the usage of discretization and count on that they take a look at a Gaussian distribution. However, this assumption based totally mostly on numerical attributes cannot hold for all the domains (or classes). Compared with naive BCs, the superior flexible BC is based totally completely on the nonparametric kernel estimation which does now not require any normality assumption and outperforms in most domains. Also, the bendy BC can shop every non-forestall feature price it sees at a few level withinside the education process.

Let f (x) be defined as a awesome opportunity density feature of one spatiotemporal pattern x of measurements assumed to be tampered with cyberattacks, and permit b f(x) be an approximate estimate of f (x) based totally mostly on n samples of pattern x. We assume that a kernel density estimation feature b fn (x) can be perfectly used to in shape the right feature f (x) of one spatiotemporal pattern x. That is to say, b fn (x) is strongly pointwise regular if b fn (x) ! f (x) is confident for all samples of the spatiotemporal pattern x. This assumption may be mathematically expressed by:

$$Pr\left(\lim_{n\to\infty}\left|\widehat{f_n}\,(x) - f\,(x)\right| < \epsilon\right) = 1, \quad \forall \epsilon : \; \epsilon > 0 \quad (3)$$

Where € is the ideal errors and can be set as any great fee that is sufficiently small. Let A be the variable denoting the template of a cyberattack instance, and allow X be a vector variable denoting the observed spatiotemporal patterns. Also, allow a represent a selected cyberattack template, and allow x represent a selected observed spatiotemporal pattern vector.

$$\arg\max_{a\in\boldsymbol{\Lambda}} Pr\left(A=a|\underbrace{\Phi_1^{\mathbb{S}},\cdots,\Phi_i^{\mathbb{S}},\cdots\Phi_{N_{\mathrm{S}}}^{\mathbb{S}}}_{Spatial\ Patterns},\underbrace{\Phi_1^{\mathbb{T}},\cdots,\Phi_j^{\mathbb{T}},\cdots\Phi_{N_{\mathrm{T}}}^{\mathbb{T}}}_{Temporal\ Patterns}\right)$$

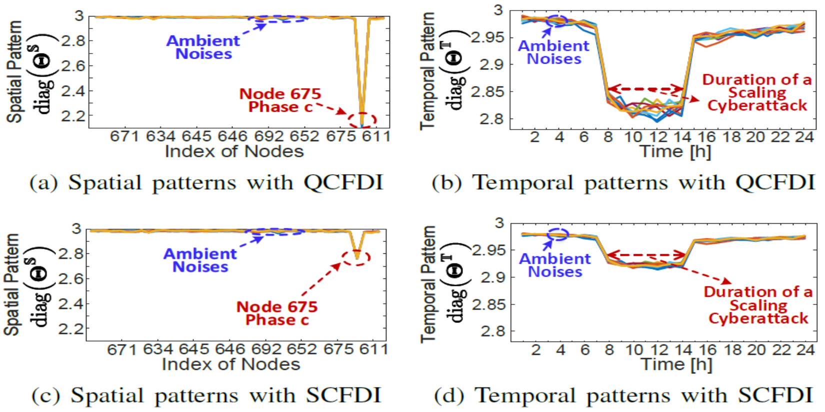
$$= \frac{\pi\left(A=a\right)\prod_{\mathbf{x}\in\boldsymbol{\Phi}} Pr\left(\mathbf{X}=\mathbf{x}|A=a\right)}{\sum_{a\in\boldsymbol{\Lambda}}\pi\left(A=a\right)\prod_{\mathbf{x}\in\boldsymbol{\Phi}} Pr\left(\mathbf{X}=\mathbf{x}|A=a\right)} \quad (4)$$

$$\Longrightarrow \arg\max_{a\in\boldsymbol{\Lambda}} \ \pi\left(A=a\right)\prod_{\mathbf{x}\in\boldsymbol{\Phi}} Pr\left(\mathbf{X}=\mathbf{x}|A=a\right) \quad (5)$$

Where Si and T i constitute the spatial and temporal patterns anticipated via way of means of GGL, respectively. NS is the wide variety of measurements withinside the spatial domain. NT is the wide variety of time windows. (A = a) is the previous chance of the attack template a. Pr() is the conditional chance function. represents the set of 4 cyberattack templates, i.e., scaling, ramping, random, and smooth-curve attacks.

Results Analysis

The uncooked load statistics is received from the Pecan Street Data port [6]. 80% of the measurement statistics in a whole year (292 days) is used for training with 28,032 samples, while 20% of those (seventy 3 days) is used for attempting out with 7,008 samples. Four cyberattack templates are simulated on each node associated with load, collectively with scaling, ramping, random, and clean curve attacks. Detailed records of cyberattack templates is described in Appendix A. Two distribution systems with thirteen and 123 buses are simulated the usage of Open DSS [7]. Active and reactive power statistics in distribution systems is concept to be inclined beneath cyberattack scenarios.



(a) Spatial patterns with QCFDI (b) Temporal patterns with QCFDI

(c) Spatial patterns with SCFDI (d) Temporal patterns with SCFDI

Fig. 2. Robustness analysis of spatiotemporal patterns using GGL against ambient noises.

To affirm the robustness of spatiotemporal patterns diagnosed via GGL, Fig. 2 shows the effects with specific ambient noises on tool measurements. Figs. 2a and 2b are with rapid changing faux data injection (QCFDI) attacks. Fig. 2a shows an example of spatial patterns with cyberattacks gift on Node 675 Phase c. Fig. 2b presents an example of temporal patterns with cyberattacks gift from 8 hour to 14 hour. As can be seen, the GGL can because it ought to be capture every spatial and temporal patterns at the same time as QCFDI attacks occur. Also, the effects are robust for specific ambient noises. Figs. 2c and second are with slowly changing faux data injection (SCFDI) attacks. The slow extrude amplitude of SCFDI attacks is set as 10% of that of QCFDI attacks. Similarly, the GGL can because it ought to be capture every spatial and temporal patterns at the same time as SCFDI attacks occur. Also, the effects are robust for specific ambient noises.

With higher TPR values. Also, TPR values are elevated with scaling attack parameters (from 0.2 to 1.0). To quantitatively take a look at the general overall performance of the advanced method, Table I compares specific detection techniques for cyberattacks withinside the IEEE 123-node test feeder. As can be seen, the flexible BC shows the largest TPR metric compared with the naive BC, SVM, and preference tree techniques. This is due to the fact the flexible BC does now not require any normality assumption and may save every non-forestall function fee it sees in some unspecified time in the future of the education process.

Method	FBC	Naïve BC	SVM	DT
TPR (%)	94.32	91.91	91.01	90.26
Accuracy (%)	94.32	92.12	92.03	91026

Table 1. Comparison of various detection methods for cyberattack

Spatiotemporal kinds of measurements have been extensively used withinside the areas of renewable forecasting and plug-in electric powered vehicles (PEVs) in ultra-modern years. Inspired thru manner of approach of this background, deploying spatiotemporal patterns for cyberattack detection has a large prospect thru manner of approach of coordinating with device gaining knowledge of techniques. Complex distribution networks can be defined as a graphical model wherein variables are associated with tremendously nonlinear purpose functions, and complex spatial and temporal relationships exist among such variables even for cyberattacks.

Since distribution systems are running based mostly on complex physical felony suggestions and rules, describing the spatiotemporal patterns thru manner of approach of device gaining knowledge of paves a way for mapping such relationships that could be significantly compromised thru manner of approach of the injected cyberattacks. For the future art work of this letter, deep gaining knowledge of techniques will be further involved. That is to say, the spatiotemporal patterns will be mapped to a linear area thru manner of approach of using the Long Short-term Memory (LSTM) network to beautify the functionality detection accuracy for cyberattacks.

In this work, we are not aiming to develop new adversary models of cyberattack templates. Inspired with the resource of the use of present adversary models for attacking automatic generation control (AGC) [9], we expect that attackers with advanced talents ought to migrate the ones adversary models to those on micro-PMU measurements in distribution systems. The cyberattack templates can be divided into four categories: scaling, ramping, random, and smooth-curve, which is probably in short described as follows. Note that this letter does now now not reason to develop new templates for cyberattacks.

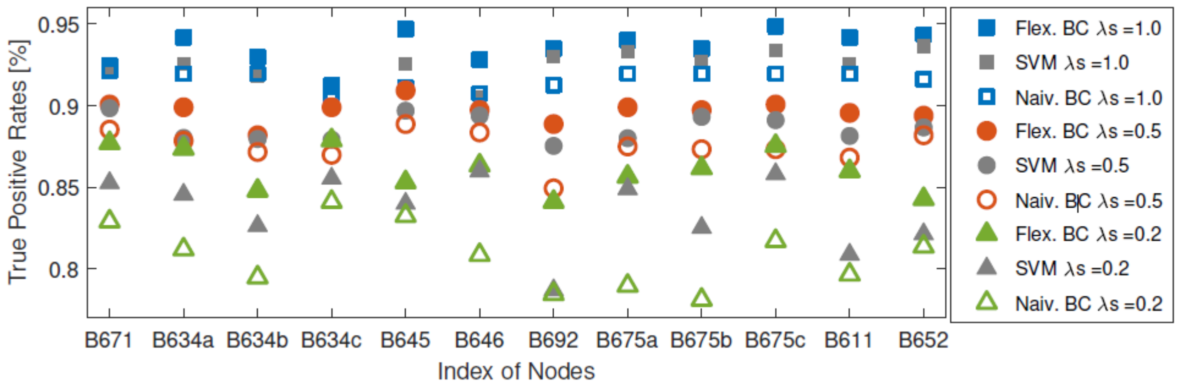
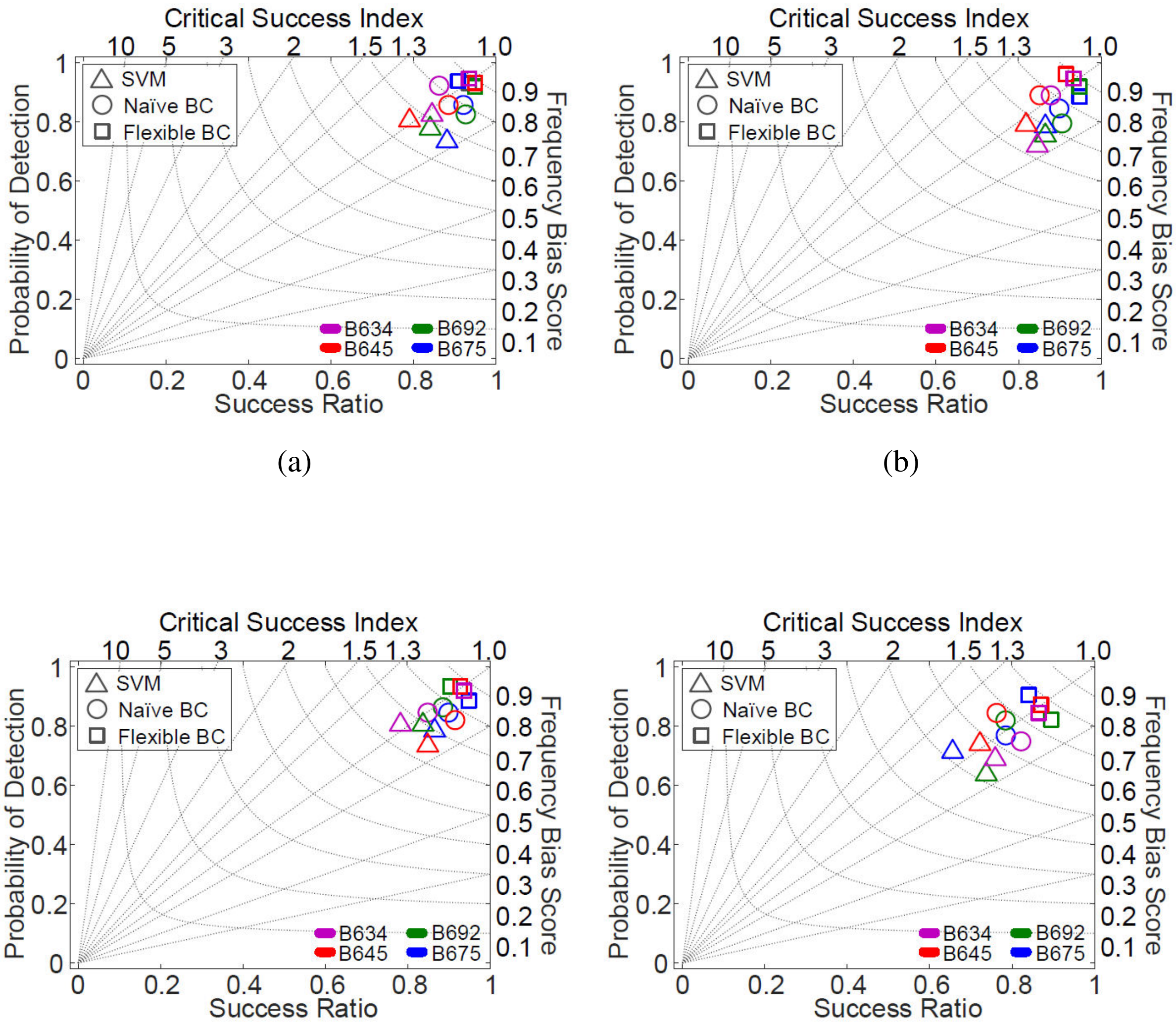


Fig 3. Scaling attack parameters comparison (λs=0.2, 0.5, and 1.0) on the IEEE 13-node test feeder.



(a)

(b)

(d)

(e)

Fig 4. Scaling (a), Ramping (b), Random (c) and smooth curve (d) attacks.

Conclusion

In this paper, we evolved a flexible ML primarily based totally cyberattack detection method through the use of method of the usage of the generalized graph Laplacian (GGL) and bendy Bayes classifiers (BCs). Spatiotemporal styles are quantitatively characterized thru manner of method of GGL, which may be compromised whilst cyberattacks occur. The bendy BCs are used for scaling spatiotemporal styles of device measurements and detecting cyberattacks online. Numerical outcomes of case studies verify the effectiveness of the advanced cyberattack detection method based mostly on machine learning techniques. Our version given accuracy of 93.3% and proved higher than different models.

References

[1] Y. Wang, Q. Chen, T. Hong, and C. Kang, “Review of smart meter data analytics: Applications, methodologies, and challenges,” IEEE Trans. Smart Grid, vol. 10, no. 3, pp. 3125–3148, May 2019.

[2] Bi, J., Luo, F., He, S., Liang, G., Meng, W., Sun, M., 2022. False data injection- and propagation-aware game theoretical approach for microgrids. IEEE Transactions on Smart Grid.

[3] M. Cui, J. Wang, A. R. Florita, and Y. Zhang, “Generalized graph Laplacian based anomaly detection for spatiotemporal microPMU data,” IEEE Trans. Power Syst., vol. 34, no. 5, pp. 3960–3963, Sep. 2019.

[4] Aslani, M., Faraji, J., Hashemi-Dezaki, H., Ketabi, A., 2022. A novel clustering-based method for reliability assessment of cyber-physical microgrids considering cyber interdependencies and information transmission errors. Applied Energy 315, 119032.

[5] H. E. Egilmez, E. Pavez, and A. Ortega, “Graph learning from data under Laplacian and structural constraints,” IEEE J. Sel. Top. Signal Process.,vol. 11, no. 6, pp. 825–841, 2017.

[6] M. Cui, J. Wang, and M. Yue, “Machine learning based anomaly detection for load forecasting under cyberattacks,” IEEE Trans. Smart Grid, vol. 10, no. 5, pp. 5724–5734, Sep. 2019.

[7] Ahmed, S., Lee, Y., Hyun, S., Koo, I., 2019. Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest. IEEE Transactions on Information Forensics and Security 14, 2765–2777.