An Unsupervised Approach to Enhance Cyber Resiliency of Power Systems Against False Data Injection Attacks on Voltage Stability

Shahriar Rahman Fahim[1,*], Rachad Atat[2], Abdulrahman Takiddin[3], Muhammad Ismail[4], Katherine R. Davis[1], and Erchin Serpedin[1]
[1] Electrical & Computer Engineering Department, Texas A&M University, College Station, TX 77843, USA
[2] Department of Computer Science and Mathematics, Lebanese American University, Beirut, Lebanon
[3] Electrical & Computer Engineering Department, Florida State University, Tallahassee, FL 32310, USA
[4] Department of Computer Science, Tennessee Tech University, Cookeville, TN 38505 USA
Email: sr-fahim@tamu.edu (S.R.F.); rachad.atat@lau.edu.lb (R.A.); a.takiddin@fsu.edu (A.T.); mismail@tntech.edu (M.I.); katedavis@tamu.edu (K.R.D.); eserpedin@tamu.edu (E.S.)

Manuscript received September 2, 2024; revised October 28, 2024; accepted November 20, 2024
*Corresponding author

***Abstract*—The digital transformation of power system introduces False Data Injection Attacks (FDIAs) on voltage stability that compromises the operational integrity of power grids. Existing detection mechanisms for FDIAs often fall short as they overlook the complexities of cyberattacks targeting voltage stability and rely on outdated models that do not capture the dynamic interplay between power system operations and potential threats. In response to these gaps, this paper proposes a novel FDIA detection method designed specifically for voltage regulation vulnerabilities, aiming to enhance the voltage stability index. The proposed method utilizes an unsupervised learning framework capable of identifying cyberattacks targeting voltage regulation. A bi-level optimization approach is put forward to concurrently optimize the objectives of both attackers and defenders in the context of voltage regulation. The effectiveness of this approach is validated through comprehensive training and testing on a variety of attack scenarios, demonstrating superior generalization across different conditions. Extensive simulations on the Iberian power system topology, with 486 buses, show that the proposed model achieves more than 93% detection rate. These results highlight the robustness and efficacy of the proposed strategy in strengthening the cyber resilience of power systems against sophisticated FDIA threats on voltage stability.**

***Index Terms*—cybersecurity, data falsification, false data injection attacks, graph autoencoder, voltage regulation, voltage stability**

I. Introduction

Modern power systems have become more advanced and efficient, but they often operate close to their stability limits with reduced security margins [1]. When these limits are exceeded, or the security margins are not maintained, the risk of large-scale blackouts increases significantly. Therefore, assessing the stability of power systems, particularly voltage stability, is crucial [2]. Voltage instability occurs when the system cannot maintain acceptable steady-state voltages across all buses under normal operations or after disturbances. This instability is primarily caused by factors such as system overloading, reactive power shortages, or equipment failures. A historical event in Egypt on April 24, 1990 [3] underscored the impact of voltage instability on power systems.

Voltage-regulating equipments, such as capacitor banks, voltage regulators, on-load tap changers, static Volt-Ampere Reactive (VAR) compensators, and smart inverters, work together to ensure voltage stability by minimizing fluctuations and system oscillations. This is typically achieved by injecting reactive power into the system. However, a shortage of reactive power can lead to voltage drops which, in turn, triggers cascading failures. Regulating devices may disconnect generators to prevent overheating, causing further reductions in reactive power. This cycle can ultimately lead to a voltage collapse. With the modernization of grids, voltage-regulating devices are increasingly managed remotely through various communication technologies. While this automation enhances grid control, it also increases the vulnerability of voltage regulation networks to cyberattacks. In False Data Injection Attacks (FDIAs), malicious actors falsify the voltage readings by making them to seem high (additive attacks), low (deductive attacks), or a blend of the two (camouflage attacks), to compromise the voltage stability index. These attacks can introduce fluctuations in the voltage levels which, in turn, disrupt the voltage stability index.

A. Related Works

Previous attack detection strategies rely on the residuals between actual and measured data [4]. When these residuals exceed a certain threshold, they indicate the possible presence of bad data. Although these methods are widely used, it has been shown that FDIAs can bypass such detectors.

To develop more robust FDIA detection strategies, recent methods have utilized the Kullback-Leibler (KL) distance [5] and a Bayesian framework [6]. However, these methods often struggle to detect FDIAs that share

the same distribution as historical measurements and are generally more effective at identifying attacks that result in abnormal system conditions.

Recently, machine learning and deep learning-based methods for detecting FDIAs have gained significant attention due to their ability to learn inherent features from data. In this context, feed-forward neural network (FNN)-based FDIA detectors have been reported to achieve accuracy levels exceeding 90% [7, 8]. Esmalifalak *et al*. [9] introduced a detection scheme using a support vector machine (SVM), which achieved an F1 score of 82%. To further enhance detection capabilities, the study in [10] introduced a variational autoencoder for anomaly detection in power grids. A comparative performance analysis in [11] showed that a deep belief network-based approach outperformed extreme learning machines and residual-based detectors. However, a limitation of these methods is their inability to fully capture the spatial relationships within sensor measurement data, as they often overlook the topological features of power grids [12].

Graph-based attack detection strategies offer a powerful solution to address the limitations of traditional deep learning models by effectively capturing both spatial and temporal features from graph-structured power system data [13]. For instance, a study in [14] showed a 4% improvement in the F1 score over a standard GNN-based detector. To detect unobservable attacks, an ARIMA-based model was introduced in [15], enabling better adaptation to sudden variations in the spectral domain. A modified multi-temporal graph Convolutional Neural Network (CNN) achieved 96% accuracy by integrating the training phases of graph convolutions and multilayer perceptions to represent node features [16]. In [17], a hybrid approach combining a graph CNN with a long-short time memory (LSTM) module also reached a 96% detection rate. A Graph Autoencoder (GAE)-based model demonstrated its effectiveness on unseen topologies, with 12% improvement over shallow detectors [18]. Comparative studies [19] further indicated that autoencoders with attention mechanisms outperform simple and variational autoencoders in detecting FDIAs and enhancing system resilience to cyberattacks. Despite these advances, most graph-based detectors are trained and tested without considering the impact on voltage stability, which is frequently affected by FDIAs.

A specialized FDIA detection algorithm for voltage stability is crucial due to the unique and complex challenges involved in maintaining voltage levels within power systems. FDIAs that target voltage measurements can cause small but critical deviations in data that traditional detectors may overlook. Even minor discrepancies in reactive power can accumulate, leading to misalignment between actual and perceived system states and potentially causing voltage collapse. This risk is heightened under stressed conditions, such as peak loads or post-fault scenarios, where the system's margin for error is already minimal. A dedicated algorithm would continuously monitor the voltage stability index and provide early warnings to prevent the system from reaching critical instability. Therefore, given the specific vulnerabilities and high stakes associated with voltage stability, a dedicated FDIA detection approach is required.

B. Contributions

The key contributions of this paper are summarized as follows.

- First, we introduce a GAE-based detector for cyberattacks on voltage regulation that captures both temporal and spatial relationships in power grid data using Chebyshev convolutional operations.
- Second, the proposed model effectively detects FDIAs, even with unseen topologies, validating its generalization and practical applicability.
- Third, we employ a bi-level optimization framework to craft cyberattacks with enhanced effectiveness and stealthiness and to create a more potent threat to the voltage regulation.
- Fourth, to showcase the efficacy of the proposed detector, we undertake comprehensive simulations, subjecting it to a range of power system attacks including targeted scenarios on random and vulnerable buses.

II. Voltage Stability Index

The voltage stability index is an indicator of power system health and operational reliability. This index is designed to reach a marginal value as the system reaches close to the instability point. To assess the stability of the overall system, we considered both the bus and line voltage stability indices [20] which will be discussed next.

A. Bus Voltage Stability Index

If V_b and V_i represent the voltage at b^{th} generator bus and i^{th} load bus, the matrix $\mathbf{F}$ can be represented in terms of the sub-matrices $\mathbf{Y}_{ii}$ and $\mathbf{Y}_{ib}$. N_g is the number of generator bus. We express the bus voltage stability index at the ith bus, Δ_B^i, as:

$$\Delta_B^i = \left|1 - \sum_{b=1}^{N_g} F_{i,b} \frac{V_b}{V_i}\right|, \tag{1}$$

In the event of cyberattacks, the Δ_B^i index can be falsely altered at various buses. The manipulated Δ_B^i index, denoted as $\tilde{\Delta}_B^i$ at the ith bus is expressed as

$$\tilde{\Delta}_B^i = \left|1 - \sum_{b=1}^{N_g} F_{ib} \frac{V_b}{\tilde{V}_i}\right|, \tag{2}$$

where $\tilde{V}_i$ indicates the false voltage measurement at bus i. Taking the average of Δ_B^i over all the buses gives the global bus voltage stability index for the whole system.

B. Line Voltage Stability Index

The bus voltages V_k and V_j at the ends of the line connecting buses i and j are related by

$$V_k = \sqrt{\left(V_j + \frac{P_{k,j}R + Q_{k,j}X_R}{V_j}\right)^2 + \left(\frac{P_{k,j}X_R - Q_{k,j}R}{V_j}\right)^2}, \tag{3}$$

where the active and reactive powers flowing from bus k to bus j are denoted by $P_{k,j}$ and $Q_{k,j}$, respectively; R is the equivalent resistance and X_R is the reactance of the

branch. The line voltage stability index $\Delta_L^{k,j}$ of the line connecting buses k and j is given by:

$$\Delta_L^{k,j} = \frac{V_k}{\sqrt{2V_j^2 + 2\left(P_{k,j}R + Q_{k,j}X_R\right)}}, \quad (4)$$

and satisfies this condition $0 < \Delta_L^{k,j} < 1$. When the system is near its stability limit, the voltage stability index approaches 1. The overall voltage stability index, Δ_o, is determined by taking the maximum value between the line voltage index Δ_L and bus voltage index Δ_B: $\Delta_o = \max\{\Delta_L, \Delta_B\}$.

III. Bi-Level Optimization Problem Formulation

In this section, we formulate a bi-level optimization problem for voltage stability in power systems involving an attacker and a defender, each with distinct objectives. The attacker aims to maximize disruption by destabilizing the system's voltage, while the defender seeks to minimize this impact through security measures. If an attacker alters the voltage measurement at a bus, the voltage deviation is given by $\Delta\mathbf{V}_a = [\Delta V_a^1, \Delta V_a^2, \times\times\times, \Delta V_a^{N_l}]$. The defender counters by using load compensation devices to inject reactive power at load buses, denoted as $\mathbf{q}_d = [q_d^1, q_d^2, \times\times\times, q_d^{N_l}]$. Here, $\mathbf{q}_d$ represents the reactive power vector that the defender uses to mitigate the attack $\Delta\mathbf{V}_a$. The utility function for the attacker, $U_a(\Delta\mathbf{V}_a, \mathbf{q}_d)$, is defined as:

$$U_a(\Delta\mathbf{V}_a, \mathbf{q}_d) = \sum_{i=1}^{N_l} P_a(h_i)\Delta_o^i, \quad (5)$$

where $P_a(h_i)$ is the probability of a successful attack at load bus i, dependent on the binary variable h_i [21]. If the attack on node i succeeds, $h_i = 1$; otherwise, $h_i = 0$. The defender's utility function, $U_d(\Delta\mathbf{V}_a, \mathbf{q}_d)$, is given by:

$$U_d(\Delta\mathbf{V}_a, \mathbf{q}_d) = -U_a(\Delta\mathbf{V}_a, \mathbf{q}_d) \quad (6)$$

The bi-level optimization problem is formulated as follows:

$$g(\Delta\mathbf{V}_a, \mathbf{q}_d) = \underset{\Delta\mathbf{V}_a}{\operatorname{argmax}}\, U_a(\Delta\mathbf{V}_a, \mathbf{q}_d) \quad (7)$$

$$f(\Delta\mathbf{V}_a, \mathbf{q}_d) = \underset{\mathbf{q}_d}{\operatorname{argmax}}\, U_d(g(\Delta\mathbf{V}_a, \mathbf{q}_d), \mathbf{q}_d) \quad (8)$$

Eq. (7) represents the attacker's upper-level objective, aiming to maximize the disruption of the voltage stability index. Given the defender's action $\mathbf{q}_d$, the attacker identifies a strategy pair, $g(\Delta\mathbf{V}_a, \mathbf{q}_d)$. Equation (8) defines the defender's lower-level objective, which seeks to maximize compensation against the attacker's actions.

IV. GAE-Based Attack Detection Scheme

The features of GAE-based attack detection framework are next reviewed.

A. Components of Graphs

An interconnected power system can be modeled as a graph, which makes GAE-based methods suitable for understanding its complex dynamics. In this graph representation, power grid buses are nodes and their connections are edges. Power grids are typically modeled as undirected, interconnected weighted graphs [14, 22]. In this paper, we define the power system graph as $\mathcal{G} = (\mathcal{N}, \mathcal{E}, \mathbf{W})$, where $\mathcal{N}$ represents the set of nodes (buses) and $\mathcal{E}$ represents the set of edges (physical lines interconnecting buses). The adjacency matrix $\mathbf{W} \in \mathbb{R}^{n\times n}$ models the weighted relationships between buses. If buses i and j are connected, the weight $\mathbf{W}_{i,j}$ is assigned to edge $e = (i, j)$. A graph representation of the considered power system is represented in Fig. 1.

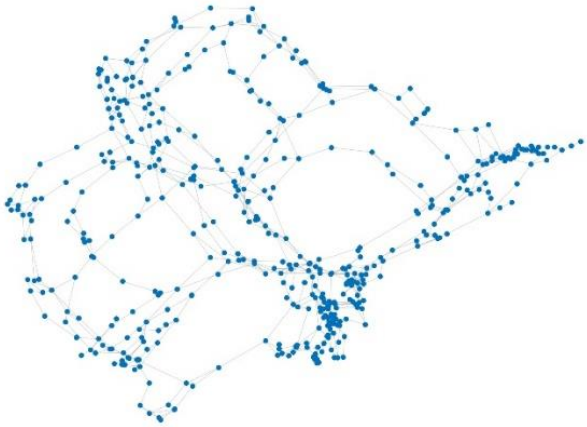


Fig 1. Graph representation of the Iberian power system.

B. Unsupervised Learning Objective

The goal is to identify deviations in input samples $\mathbf{X}$, indicating the presence of cyberattacks in power systems. The input samples consist of temporal measurements of active and reactive power, $[\mathbf{P}_t, \mathbf{Q}_t] \in \mathbb{R}^{n\times 2}$ at the t th timestamp. As shown in Fig. 2, the input data passes through graph encoder layers l_E, which produce a latent representation at layer l_H, followed by graph decoder layers l_D. The graph encoder and decoder functions are $E_{\mathcal{G}} = f_E(\mathbf{X})$ and $D_{\mathcal{G}} = f_D(\mathbf{X})$, respectively. The objective is to minimize the reconstruction error between the original input and its reconstruction:

$$\min_{\{\mu\}} \mathcal{C}\left(\mathbf{X}, f_D(f_E(\mathbf{X}))\right), \quad (9)$$

where $\{\mu\}$ represents the training parameters, and the cost function $\mathcal{C}(\cdot)$ is the mean squared error measuring the difference between $f_D(f_E(\mathbf{X}))$ and $\mathbf{X}$.

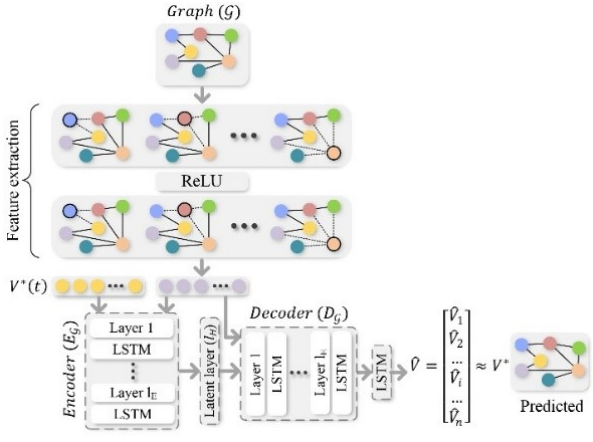


Fig. 2. Architecture of the proposed GAE.

C. Chebyshev Convolution Operation

During each training stage, the spectral graph convolution of a signal $\boldsymbol{\sigma} \in \mathbf{X}$ is defined as $\mathbf{U}\boldsymbol{\psi}_\theta \mathbf{U}^T\boldsymbol{\sigma}$, where $\mathbf{U}$ contains the eigenvectors of the normalized Laplacian $\mathbf{L} = \mathbf{U}\boldsymbol{\Omega}\mathbf{U}^T$, $\boldsymbol{\psi}_\theta = \text{diagonal}(\theta)$ is the spectral filter, and $\theta \in \mathbb{R}^n$ is the parameter vector in the Fourier domain. The diagonal matrix $\boldsymbol{\Omega}$ holds the non-negative eigenvalues λ of $\mathbf{L}$, and $\mathbf{U}^T\boldsymbol{\sigma}$ represents the Fourier transform of $\boldsymbol{\sigma}$. Later a polynomial approximation is introduced as, $H_{\boldsymbol{\gamma}}(\boldsymbol{\Omega}) = \sum_{k=0}^{m} \gamma_k \Omega^k$, where $\boldsymbol{\gamma} = (\gamma_1, \gamma_2, \times \times \times, \gamma_m)$ are the coefficients for an *m*-order polynomial. To enhance training stability, a truncated Chebyshev polynomial expansion $N_m(\tilde{\boldsymbol{\Omega}})$ is applied [23]:

$$H_{\boldsymbol{\gamma}}(\boldsymbol{\Omega}) = \sum_{k=0}^{m} \gamma_k N_k(\tilde{\boldsymbol{\Omega}}), \tag{10}$$

where $\tilde{\boldsymbol{\Omega}} = 2\boldsymbol{\Omega}/\lambda - \mathbf{I}$. The Chebyshev polynomials are recursively defined as $N_m(p) = 2pN_{m-1}(p) - N_{m-2}(p)$, with $N_0 = 1$ and $N_1 = p$. The filtering process is:

$$H_{\boldsymbol{\gamma}}(\mathbf{L})\boldsymbol{\sigma} = \sum_{k=0}^{m} \gamma_k N_k(\tilde{\mathbf{L}})\boldsymbol{\sigma}, \tag{11}$$

where $\tilde{\mathbf{L}} = 2\mathbf{L}/\lambda - \mathbf{I}$. The complexity is $\mathcal{O}(m|\mathcal{E}|)$, and with Chebyshev polynomials limited to the *m*th order, the convolutions are localized to *m* hops.

D. GAE Architecture

The architecture of the proposed GAE model is depicted in Fig. 2. Each element of its architecture is discussed next.

1) Graph encoder $E_{\mathcal{G}}$

The graph encoder has l_E Chebyshev graph convolutional layers. The inputs to the graph convolutional layers or the number of channels in a hidden encoding layer l_E is indicated by N_c. If b^{l_E} denotes the bias of layer l_E and $*_{\mathcal{G}}$ represents the graph convolutional operator. The result is the output tensor, X^{l_E} denoted as,

$$X^{l_E} = \text{ReLU}\left(\gamma_m(*_{\mathcal{G}})X^{l_E-1} + b^{l_E}\right) \tag{12}$$

To extract the temporal relationships from the time-series signal, we incorporate an LSTM unit that facilitates the modeling of recurrent information flows. An LSTM cell consists of the input $i_{l_E}^t$, output $o_{l_E}^t$, and forget gate $f_{l_E}^t$. Inside an LSTM unit, there exists two distinct states: i) the cell state $C_{l_E}^t$, and ii) the LSTM output or hidden state $H_{l_E}^t$.

2) Graph decoder $D_{\mathcal{G}}$

The main aim of the graph decoder is to produce an output $\mathbf{V}^*$ that closely resembles the input $\mathbf{X}$. The reconstruction error is measured via $\eta = \|\mathbf{V}^* - \mathbf{X}\|^2$. In the same vein as the graph encoder, the outputs of the graph decoder are sequentially fed to the LSTM that processes time-evolving graph features. The cell state of the graph decoder-LSTM is regulated by $i_{l_D}^t$, $o_{l_D}^t$, and $f_{l_D}^t$, which stand for the input, output, and forget gates, respectively.

V. Threat Modeling and Data Generation

A. Threat Model

If the voltage measurement at bus i and timestamp t is denoted as V_i^t, then the true voltage measurement, $V_{\text{true},i}^t$ should align with the measured voltage, $V_{m,i}^t$ at control end (i.e., $V_{\text{true},i}^t = V_{m,i}^t$). The tampered voltage measurement may contain false data values. The attack functions during different attack scenarios are represented as

$$\begin{cases} V_{\text{false},i}^t = V_{\text{true},i}^t + \Delta V_i^t \\ V_{\text{false},i}^t = V_{\text{true},i}^t - \Delta V_i^t \\ V_{\text{false},i}^t = V_{\text{true},i}^t + e\Delta V_i^t - (1-e)\Delta V_i^t, \end{cases}$$

where ΔV_i^t denotes the maliciously inserted data by the adversary, and e denotes a binary variable with a value of 1 indicating an additive attack and 0 representing a deductive attack. The attack functions incorporate additive, deductive, and combined attacks.

B. Strategies for Attacks

1) Random node attacks

These attacks randomly target r buses from a total of N_l, creating $N_l!/(r!\,(N_l - r)!)$ possible subsets. Such randomness can lead to severe voltage instability, especially if affected buses are not restored promptly.

2) Vulnerable nodes attacks

Vulnerability refers to a power node's likelihood of being a weak point in the system. Attacks on such nodes can cause significant voltage instability. We evaluate vulnerability by assigning scores to nodes based on electrical and topological metrics to identify the most vulnerable buses. We use the Analytical Hierarchical Process (AHP) to determine weights for each metric, calculate scores for electrical and topological vulnerabilities, and combine these to determine an overall vulnerability score.

C. Data Generation

To generate the normal time-series voltage data, we perform power flow analysis using Newton's method in the MATLAB MATPOWER toolbox. This toolbox facilitates the calculation of system voltages, currents, and both real and reactive power flows.

D. Hyperparameter Optimization

We use a sequential grid search to optimize the hyperparameters for the proposed and benchmark detectors. The optimal hyperparameters for CNN, FNN, LSTM, GCNN, and GNN are:

$$\begin{aligned} \boldsymbol{\mathcal{H}}_{\text{CNN}} &= \{4, 32, 0.4, \text{Rmsprop}, 5, \text{Relu}\}, \\ \boldsymbol{\mathcal{H}}_{\text{FNN}} &= \{4, 32, 0, \text{Adam}, \text{N/A}, \text{Relu}\}, \\ \boldsymbol{\mathcal{H}}_{\text{LSTM}} &= \{3, 32, 0.2, \text{Adam}, \text{N/A}, \text{Relu}\}, \\ \boldsymbol{\mathcal{H}}_{\text{GCNN}} &= \{5, 32, 0.2, \text{Rmsprop}, 4, \text{Relu}\}, \\ \boldsymbol{\mathcal{H}}_{\text{GAN}} &= \{6, 64, 0.2, \text{Adam}, 5, \text{Relu}\}. \end{aligned}$$

For the ARIMA model, the optimal differencing degree and moving average are 1 and 0. The SVM model's optimal gamma, kernel, and regularization are auto, sigmoid, and 1.

E. Performance Evaluation Metrics

The detection performance of the proposed FDIA detector is evaluated using three metrics: Detection Rate (DR), $\mathrm{DR} = \frac{TP}{TP+FN}$; False Alarm Rate (FAR), $\mathrm{FAR} = \frac{FP}{FP+TN}$; and Accuracy (ACC), $\mathrm{ACC} = \frac{TP+TN}{TP+TN+FP+FN}$. Here, TP, TN, FP, and FN denote the number of true positives, true negatives, false positives, and false negatives, respectively.

VI. Experimental Evaluations

In this study, three different attack types are considered: additive, deductive, and camouflage attacks. For the latter attack strategy, both additive and deductive attacks are chosen in equal proportions. For each attack scenario, 5, 10, 15, and 20% attack injection levels are chosen. On average the proposed model achieves 98.11% accuracy, 98.76% detection rate, and 8.13% false alarm rate.

A. Performance Against Random Attacks on Buses

The proposed model's detection performance against random buses attacks is depicted in Table I. The results reveal that as the injection level of the attack increases, the effectiveness of the detection decreases. This performance drop may be due to the increased likelihood of false positives.

B. Performance Against Attacks on Vulnerable Buses

The performance of the proposed model for the mentioned attack strategy is presented in Table II. From the table, it is observed that for each test case, the model reports relatively lower accuracy compared to the random node attacks. However, the model achieves more than 93% accuracy across the attack scenarios.

Table I: Performance Against Random Node Attacks

Attack type	Performance Metric	Injection levels			
		5%	10%	15%	20%
Additive	DR	91.18	99.07	98.17	96.40
	FAR	6.48	8.28	9.97	10.79
	ACC	98.87	98.77	97.88	95.80
Deductive	DR	98.10	97.33	96.88	94.47
	FAR	8.24	9.63	10.99	12.98
	ACC	97.03	97.09	96.50	94.61
Combined	DR	97.15	95.58	94.97	92.90
	FAR	10.38	10.93	12.80	13.72
	ACC	95.22	95.58	95.38	93.54

Table II: Performance Against Vulnerable Node Attacks

Attack type	Performance Metric	Injection levels			
		5%	10%	15%	20%
Additive	DR	98.31	97.78	97.01	95.88
	FAR	6.51	8.27	10.11	10.83
	ACC	98.07	97.31	96.49	94.73
Deductive	DR	98.22	97.67	96.99	95.75
	FAR	6.58	8.37	9.95	11.33
	ACC	98.00	97.17	96.37	94.56
Combined	DR	97.50	97.03	95.91	94.64
	FAR	9.56	10.22	11.13	12.66
	ACC	97.25	96.41	95.12	93.98

VII. Conclusions

This study presents a GAE-based FDIA detection framework dedicated to voltage regulation, evaluating its effectiveness against various attack types and injection levels. The proposed detector integrates an autoencoder with Chebyshev graph convolution recurrent layers to capture spatial and temporal correlations in measurement data. Simulation results show that the proposed model achieves up to 93.80% accuracy, with an average 20% improvement in ACC compared to benchmark detectors. Developing a generalized cyberattack detection scheme is suggested for future research.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Shahriar Rahman Fahim, Rachad Atat conducted the research and wrote the paper. Abdulrahman Takiddin collected the data. Muhammad Ismail, Katherine R. Davis, and Erchin Serpedin reviewed and validated the work. All authors had approved the final version.

Funding

This work is supported by NSF EPCN Awards 2220346 and 2220347.

References

[1] T. Hathiyaldeniye, U. D. Annakkage, N. Pahalawaththa, and C. Karawita, "A comparison of inverter control modes for maintaining voltage stability during system contingencies," *IEEE Open Access Journal of Power and Energy*, vol. 9, pp. 55–65, Jan. 2022.

[2] P. Kessel and H. Glavitsch, "Estimating the voltage stability of a power system," *IEEE Trans. on Power Delivery*, vol. 1, no. 3, pp. 346–354, 1986.

[3] S. A. Adegoke and Y. Sun, "Power system optimization approach to mitigate voltage instability issues: A review," *Cogent Engineering*, vol. 10, no. 1, #2153416, 2023.

[4] A. Sayghe, Y. Hu, I. Zografopoulos, X. Liu, R. G. Dutta, Y. Jin, and Konstantinou, "Survey of machine learning methods for detecting false data injection attacks in power systems," *IET Smart Grid*, vol. 3, no. 5, pp. 581–595, 2020.

[5] R. Moslemi, A. Mesbahi, and J. M. Velni, "A fast, decentralized covariance selection-based approach to detect cyber attacks in smart grids," *IEEE Trans. on Smart Grid*, vol. 9, no. 5, pp. 4930–4941, 2017.

[6] M. Zhang, C. Shen, N. He, S. Han, Q. Li, Q. Wang, and X. Guan, "False data injection attacks against smart gird state estimation: Construction, detection and defense," *Science China Technological Sciences*, vol. 62, no. 12, pp. 2077–2087, 2019.

[7] D. Xue, X. Jing, and H. Liu, "Detection of false data injection attacks in smart grid utilizing elm-based ocon framework," *IEEE Access*, vol. 7, pp. 31762–31773, 2019.

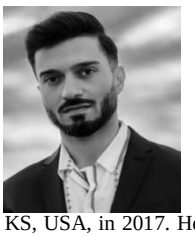
[8] E. M. Ferragut, J. Laska, M. M. Olama, and O. Ozmen, "Real-time cyber-physical false data attack detection in smart grids using neural networks," in *Proc. of* 2017 *Int. Conf. on Computational Science and Computational Intelligence (CSCI)*. IEEE, 2017. doi: 10.1109/CSCI.2017.1

[9] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1644–1652, 2014.

[10] R. Zheng, J. Gu, Z. Jin, H. Peng, and Y. Zhu, "Load forecasting under data corruption based on anomaly detection and combined

robust regression," *International Trans. on Electrical Energy Systems*, vol. 30, no. 7, #e12103, 2020.
[11] Y. Li and Y. Wang, "False data injection attacks with incomplete network topology information in smart grid," *IEEE Access*, vol. 7, pp. 3656–3664, 2018.
[12] 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. on Smart Grid*, vol. 11, no. 3, pp. 2218–2234, 2019.
[13] B. L. Nguyen, T. V. Vu, T.-T. Nguyen, M. Panwar, and R. Hovsapian, "Spatial-temporal recurrent graph neural networks for fault diagnostics in power distribution systems," *IEEE Access*, vol. 11, pp. 46039-46050, May 2023.
[14] O. Boyaci, A. Umunnakwe, A. Sahu, M. R. Narimani, M. Ismail, K. R. Davis, and E. Serpedin, "Graph neural networks based detection of stealth false data injection attacks in smart grids," *IEEE Systems Journal*, vol. 16, no. 2, pp. 2946–2957, 2021.
[15] O. Boyaci, M. R. Narimani, K. R. Davis, M. Ismail, T. J. Overbye, and E. Serpedin, "Joint detection and localization of stealth false data injection attacks in smart grids using graph neural networks," *IEEE Trans. on Smart Grid*, vol. 13, no. 1, pp. 807–819, 2021.
[16] Y. Han, H. Feng, K. Li, and Q. Zhao, "False data injection attacks detection with modified temporal multi-graph convolutional network in smart grids," *Computers and Security*, vol. 124, #103016, 2023.
[17] Y. Zhang, J. Wang, and B. Chen, "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach," *IEEE Trans. on Smart Grid*, vol. 12, no. 1, pp. 623–634, 2020.
[18] A. Takiddin, M. Ismail, U. Zafar, and E. Serpedin, "Robust electricity theft detection against data poisoning attacks in smart grids," *IEEE Trans. on Smart Grid*, vol. 12, no. 3, pp. 2675–2684, 2020.
[19] A. Takiddin, M. Ismail, U. Zafar, and E. Serpedin, "Deep autoencoder-based anomaly detection of electricity theft cyberattacks in smart grids," *IEEE Systems Journal*, vol. 16, no. 3, pp. 4106–4117, 2022.
[20] X. Ancheng, L. Ruihuang, L. Mingkai, J. H. Chow, B. Tianshu, Y. Ting, and P. Tianjiao, "On-line voltage stability index based on the voltage equation of transmission lines," *IET Generation, Transmission and Distribution*, vol. 10, no. 14, pp. 3441–3448, 2016.
[21] L. An, A. Chakrabortty, and A. Duel-Hallen, "A stackelberg security investment game for voltage stability of power systems," in *Proc. of* 2020 *59th IEEE Conf. on Decision and Control*, 2020, pp. 3359–3364.
[22] A. Takiddin, R. Atat, M. Ismail, O. Boyaci, K. R. Davis, and E. Serpedin, "Generalized graph neural network-based detection of false data injection attacks in smart grids," *IEEE Trans. on Emerging Topics in Computer Intelligence*, vol.7, no. 3, pp. 618–630, 2023.
[23] M. Defferrard, X. Bresson, and P. Vandergheynst, "Convolutional neural networks on graphs with fast localized spectral filtering," in *Proc. of the 30th Int. Conf. on Neural Information Processing Systems*, 2016, pp. 3844–3852.

Shahriar Rahman Fahim received the B.Sc. degree in electrical and electronic engineering (EEE) from the Rajshahi University of Engineering and Technology, Bangladesh in 2020. He completed his M.Sc. study in EEE from American International University-Bangladesh. He is currently pursuing a Ph.D. degree in electrical and computer engineering at Texas A&M University, College Station, USA with a focus on cybersecurity, machine learning, and the protection of modern electrified transportation systems.



Rachad Atat received the B.E. degree (Hons.) in computer engineering from Lebanese American University, Beirut, Lebanon, in 2010, the M.Sc. degree in electrical engineering from the King Abdullah University of Science and Technology (KAUST), Thuwal, Saudi Arabia, in 2012, and the Ph.D. degree (Hons.) in electrical engineering from the University of Kansas (KU), Lawrence, KS, USA, in 2017. He is currently a post-doctoral research associate at Texas A&M University at Qatar, working on dynamic metering allocation with integrated cybersecurity measures in smart grids.

Abdulrahman Takiddin received the B.Sc. (Hons.) degree in information systems from Carnegie Mellon University, Pittsburgh, PA, USA, in 2014, the M.Sc. degree in data analytics from Hamad Bin Khalifa University, Doha, Qatar, in 2020, and the Ph.D. degree in electrical engineering from Texas A&M University, College Station, TX, USA, in 2024. He is currently an assistant professor of Electrical and Computer Engineering at the FAMU-FSU College of Engineering, Florida State University, Tallahassee, FL, USA. His research interests include machine learning, cyber-physical systems, smart grid, smart vehicles, and security.

Muhammad Ismail received the B.Sc. (Hons.) and M.Sc. degrees in electrical engineering (electronics and communications) from Ain Shams University, Cairo, Egypt, in 2007 and 2009, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2013. He is the director of the Cybersecurity Education, Research, and Outreach Center (CEROC) and an Associate Professor with the Department of Computer Science, Tennessee Technological University, Cookeville, TN, USA. He was a co-recipient of the best paper awards in the IEEE ICC 2014, the IEEE GLOBECOM 2014, the SGRE 2015 and 2024, the Green 2016, the IEEE IS 2020, and the Best Conference Paper Award from the IEEE Communications Society Technical Committee on Green Communications and Networking for his publication in IEEE ICC 2019. He is a Track chair in the IEEE Globecom 2024. He has been a technical reviewer of several IEEE conferences and journals.

Katherine Davis (Senior Member, IEEE) received the B.S. degree from The University of Texas at Austin, Austin, TX, USA, in 2007, and the M.S. and Ph.D. degrees from the University of Illinois at Urbana–Champaign, Champaign, IL, USA, in 2009 and 2011, respectively, all in electrical engineering. She is currently an assistant professor of electrical and computer engineering with Texas A&M University.

Erchin Serpedin is currently a full professor with the Electrical and Computer Engineering Department, Texas A&M University at College Station, College Station, TX, USA. His research interests include signal processing, machine learning, artificial intelligence, cyber security, smart grids, and wireless communications. Dr. Serpedin was an associate editor for more than 12 journals, including journals, such as IEEE transactions on information theory, IEEE transactions on signal processing, IEEE transactions on communications, IEEE signal processing letters, IEEE communications letters, IEEE transactions on wireless communications, IEEE signal processing magazine, Signal Processing (Elsevier), Physical Communication (Elsevier), and EURASIP Journal on Advances in Signal Processing.