Generalized FDIA Detection in Power Dependent Electrified Transportation Systems

Shahriar Rahman Fahim[1], Rachad Atat[2], Cihat Kececi[1], 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]Electrical & Computer Engineering Department, Texas A&M University at Qatar, Doha 23874, Qatar;
[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; rachad.atat@qatar.tamu.edu; kececi@tamu.edu; a.takiddin@fsu.edu; mismail@tntech.edu; katedavis@tamu.edu; eserpedin@tamu.edu

***Abstract*—The increasing popularity of electric vehicles (EVs) has strengthened the integration between power and transportation networks. Amidst the rising trend of interconnecting power and transportation networks, there has been a surge in attacks targeting power systems, specifically those capable of disrupting charging services. Existing studies on identifying false data injection attacks (FDIAs) are insufficient in safeguarding coupled power-dependent electrified transportation networks for several reasons: (a) they are primarily designed for power networks only, (b) they does not consider the influence of cyber attacks on charging satisfaction rates, and (c) they lack adaptability/do not generalize well to various topological configurations. To overcome these shortcomings, this paper introduces a comprehensive FDIA detection scheme that takes into account the interconnected nature of power-transportation infrastructures, eventually improving the charging user satisfaction rates. Toward this objective, we develop a defense strategy based on a graph autoencoder (GAE) that extracts spatio-temporal features from the intertwined data, thereby providing increased resilience against FDIAs. Furthermore, our model undergoes training on diverse power system topologies and various attack scenarios, ensuring improved generalization capabilities. Simulations were conducted on two types of power systems: one with 2000 buses and another with 30 buses, featuring 360 and 35 charging stations (CSs) respectively. When subjected to unseen data, our model achieved an impressive 98.3% detection rate, marking a significant enhancement of 15% to 30% compared to benchmark strategies. This highlights the efficacy of our proposed method in adequately tackling the challenges associated with detecting FDIAs on interconnected power and transportation networks.**

***Index Terms*—Transportation network, Electric vehicles, Graph neural network, Coupled system, and Power system.**

I. Introduction

In recent years, the excessive consumption of fossil fuels has contributed to a steady increase in global greenhouse gas emissions, prompting heightened attention from nations toward climate change-related issues. The transportation sector stands as the major contributor to anthropogenic greenhouse gas emissions in the United States, accounting for 28% of the worldwide total [1]. In efforts to reduce the reliance of the transportation sector on fossil fuels, transportation electrification has emerged as a key strategy. Recognizing these benefits, the interdependency between the power and transportation systems strengthens with the adoption of EVs on a global scale, spanning regions such as the US, EU, and China [2]. Moreover, modern cyber-physical power systems rely on a large amount of metered data exchanged within the power grid for operational or situational purposes. Consequently, ensuring the authenticity of this collected data is imperative for maintaining the stability and reliability of the system. A significant threat to data integrity arises from FDIAs, where malicious entities manipulate the sensor measurement data [3]. These attacks have the potential to influence operational decisions that lessen the customer satisfaction rate. Hence, recent studies have focused on formulating intelligent defense strategies that can effectively detect such attacks.

The CSs draw power from the power buses for efficient charging of the EVs. Thus, the EV user experience is influenced by the electric power availability on a bus. During FDIAs, the attackers manipulate the power readings to make them appear higher (additive attacks), lower (deductive attacks), or a blend of both (camouflage attacks). In additive attacks, the attacker creates a false perception of abundant capacity. Conversely, in deductive attacks, the attacker portrays a deceptive impression of inadequate power. These falsified data induce charging uncertainty and decrease charging satisfaction rates significantly. Camouflage attacks result in fluctuation of charging power demands across different buses. This paper aims to develop a novel FDIA detection scheme for power-dependent electrified transportation networks and to evaluate the impact of cyberattacks on EV-users' satisfaction rate.

A. Literature Review

The growing complexity of contemporary power systems has lead to a shift in the area of power attack detection from classical model-based approaches to more dynamic and versatile machine learning (ML)-based approaches. Classical model-based approaches operate under the assumption that the system behavior is predicted precisely by a mathematical model. For example, the state estimation-based detection strategy was employed in [4] and [5], and the models used compare the estimated states with the actual measurements to detect the anomalies. Reference [6] proposed a decentralized model-based approach based on the maximum likelihood principle.

In [7] the authors proposed an extended Kalman filter interval state estimation technique. Due to the complex couplings between the power and transportation systems, capturing all the system dynamics is often challenging and impractical.

Data-driven ML-based approaches have emerged as an effective and viable alternative to classical model-based approaches. ML approaches have demonstrated varying levels of success. A feed-forward neural network (FNN)-based attack detector showed over 90% detection rate [8]. A generative adversarial network model with an integrated autoencoder reported a detection performance of 96.2% [9]. In [10], a combination of the Kalman filter and recurrent neural network (RNN) achieved a detection rate of 96%. A convolutional neural network (CNN) in conjunction with a Kalman filter achieved 99% detection accuracy [11]. Despite their high detection rates, ML approaches often overlook the topological and physical characteristics of power grids.

A power distribution system can be formally represented as a graph whose nodes capture the power grid's buses and its edges represent the power lines [12]. Such graph representation facilitates modeling and analysis of complex topologies, and capturing of spatial and temporal dependencies essential for tracking the ever-changing dynamics of power systems. Within the graph signal processing framework, an auto-regressive moving average (ARIMA) model combined with a graph filter was proposed in [13] to detect stealthy attacks on power systems. Reference [14] proposed a modified temporal multi-graph convolutional network that achieves 96% accuracy across different power system topologies. In [9], the authors combined graph convolution with long short-term memory (LSTM) and achieved 96% detection accuracy. In reference [15], a graph autoencoder (GAE)-based approach was introduced for identifying cyber attacks within network topologies that were not previously encountered, showing a 12% improvement over shallow detectors.

Although the above mentioned GNN-based detectors present certain advantages, their domain of applicability is limited since they are exclusively built for electric power systems. This work extends the area of applicability of FDIA detectors to the more general framework of coupled power and transportation systems.

B. Contributions

The major contributions of this paper are outlined next:

- First, we propose a detection strategy using graph autoencoder (GAE) for coupled electrified transportation systems that effectively extracts topological features from both systems through Chebyshev graph convolution operation.
- Second, the proposed approach offers improved generalizability as it is trained on multiple system topologies. The enlarged training ensures adaptability and robustness in real-world scenarios.
- Third, we evaluate the performance of the proposed approach against various attack types, including additive, deductive, and camouflage attacks. We also assess scenarios where attackers have either a limited or comprehensive knowledge of the coupled system, enabling the identification of network vulnerabilities.
- Fourth, we analyze the impact of these cyberattacks on EV users' charging satisfaction rates using data from 2,000 and 30 bus power systems with 360 and 35 allocated CSs, respectively.

II. The Integrated Power-Transportation System Modeling

Given the intrinsic graph-like configuration of power grids, leveraging GNN-based strategies is promising for developing efficient FDIA detector. However, the asymmetric nature of directed graphs can hinder information flow and limit the learning ability of GNNs, particularly at the peripheral grid areas [16]. To address this issue, we represent power systems as undirected weighted connected graphs, $\mathcal{G} = (\mathbf{V}, \mathbf{E}, \mathbf{W})$, where $\mathbf{V} = \{1, 2, .., B\}$ signifies the set of nodes or buses while B indicates the total count of power system buses. $\mathbf{W} \in \mathbb{R}^{B \times B}$ and $\mathbf{E}$ represent the adjacency matrix and the set of edges or power lines joining two buses, respectively. If there is a link between buses i and j, $\mathbf{W}_{ij}$ is set to 1, otherwise it is set to 0.

The considered transportation networks comprises 360 and 35 CSs, respectively, each CS being uniquely localized via precise geographic coordinates. To establish an effective and meaningful coupling between the two systems, we overlay the power and transportation networks and align them based on their respective positions. Then, we connect the CSs to the power buses based on the shortest distance between them which ensures a seamless integration that optimizes efficiency and functionality. Fig.1 illustrates the coupling of power and transportation network.

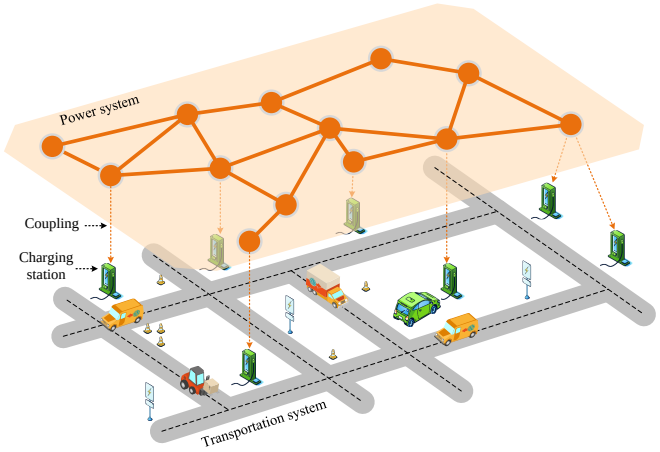

Fig. 1. Power-dependent electrified transportation system.

III. Threat Modeling

The attack functions and strategies are next discussed.

A. Attack Functions

Herein paper, we consider three distinct attack types: i) additive attacks, ii) deductive attacks, and iii) combined attacks. Denote the measured power at bus i and timestamp t by P_i^t. The true power measurement, $P_{\text{true},i}^t$, should align with the field power measurement, $P_{\text{m},i}^t$, at the control center (i.e., $P_{\text{true},i}^t = P_{\text{m},i}^t$). The attack functions during different attack scenarios are formally expressed as:

Attack functions

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

where ΔP_i^t denotes the stealthily inserted power value by the adversary and e represents a binary variable taking the values 1 or 0, indicating an additive or deductive attack, respectively.

B. Attack Strategies

1) Attacks on random power nodes (RNA): these attacks entail a random selection of power nodes as targets. These attacks assume randomly selecting a subset of r buses from a total of B buses (where $r \leq B$). The number of possible subsets is $\frac{B!}{r!(B-r)!}$. These attacks have the potential to disrupt the system operation which, in turn, lessens user satisfaction rate.

2) Attacks at the most vulnerable power nodes (VNA): Vulnerability indicates the potential of a power node to act as a critical failure point, i.e., a vulnerable location where an attack could cause significant harm to the entire system. Vulnerability assessment process assigns vulnerability scores to power buses that will later be used to formulate strategies targeting the most vulnerable buses. The vulnerability is influenced by both their topological characteristics and power flow of a system. We consider a comprehensive set of metrics to encompass both the topological and electrical aspects of the power grid [17]–[19]. The weight of these vulnerability metrics is determined via the Analytical Hierarchy Process (AHP) [20], where pairwise comparisons are conducted to assess the comparative significance of each metric.

IV. GAE BASED ATTACK DETECTION SCHEME

This section describes the proposed GAE architecture. We formulate the FDIA detection task as a classification problem where the aim is to classify input samples $\boldsymbol{X}$ into two distinct categories, one indicating the presence and the other the absence of cyber attacks. The input samples consist of the temporal measurement data for active and reactive powers, $[\boldsymbol{P}_t, \boldsymbol{Q}_t] \in \mathbb{R}^{n\times 2}$ at the t^{th} timestamp. Fig. 2 depicts the architecture of the proposed model. The objective is to learn the data patterns from benign input samples and measure the reconstruction error η while reconstructing. The graph encoder and decoder functions are denoted by $E_{\mathcal{G}} = f_E(\boldsymbol{X})$ and $D_{\mathcal{G}} = f_D(\boldsymbol{X})$, respectively. The objective function of the proposed model is given by:

$$\min_{\{\mu\}} \mathcal{C}\left(\boldsymbol{X}, f_D\left(f_E(\boldsymbol{X})\right)\right). \tag{2}$$

The essential components of the considered GAE architecture are next presented.

A. Chebyshev Convolution Operation

During the training period, the spectral graph convolution with input signal $\boldsymbol{\sigma} \in \boldsymbol{X}$ is performed as $\boldsymbol{U}\boldsymbol{\psi}_\theta\boldsymbol{U}^T\boldsymbol{\sigma}$. Matrix $\boldsymbol{U}$ incorporates the eigenvectors of normalized Laplacian $\boldsymbol{L} = \boldsymbol{U}\boldsymbol{\Omega}\boldsymbol{U}^T$. The spectral filter $\boldsymbol{\psi}_\theta = \text{diagonal}(\theta)$ incorporates the parameter vector $\theta \in \mathbb{R}^n$ in the Fourier domain. The diagonal matrix $\boldsymbol{\Omega}$ captures the non-negative eigenvalues λ of $\boldsymbol{L}$. The Fourier transformation of $\boldsymbol{\sigma}$ is performed through $\boldsymbol{U}^T\boldsymbol{\sigma}$. Spatially localized filters extract features from a particular region of interest, rather than performing filtering operations over the entire input sequence. This selectivity is implemented via the polynomial: $H_{\boldsymbol{\gamma}}(\boldsymbol{\Omega}) = \sum_{k=0}^{m} \gamma_k \boldsymbol{\Omega}^k$, where $\boldsymbol{\gamma} = (\gamma_0, \gamma_1, ..., \gamma_m)$ represents the vector of coefficients that the model seeks to learn for the m^{th}-order polynomial. The polynomial filtering is expressed as

$$\boldsymbol{U}H_{\boldsymbol{\gamma}}(\boldsymbol{\Omega})\boldsymbol{U}^\top\boldsymbol{\sigma} = H_{\boldsymbol{\gamma}}(\boldsymbol{L})\boldsymbol{\sigma} = \sum_{k=0}^{m} \gamma_k N_k(\tilde{\boldsymbol{L}})\boldsymbol{\sigma}, \tag{3}$$

where $\tilde{\mathbf{L}} = 2\boldsymbol{L}/\lambda - \mathbf{I}$. The computational complexity of the filtering operation is $\mathcal{O}(m|\mathbf{E}|)$.

1) Graph Encoder $E_{\mathcal{G}}$: The graph encoder has l_E Chebyshev graph convolutional layers. This layer extracts the spatial characteristics from the network via graph convolution operations, bias addition, and the application of the ReLU activation function. The resulting output is the tensor:

$$\boldsymbol{X}_{l_E} = \text{ReLU}\left(\gamma_m *_{\mathcal{G}} \boldsymbol{X}_{l_E-1} + \boldsymbol{b}_{l_E}\right). \tag{4}$$

Vector $\boldsymbol{b}_{l_E}$ denotes the bias at layer l_E and $*_{\mathcal{G}}$ represents the graph convolutional operator. The bias in the ReLU activation function promotes nonlinear processing.

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 $f_{l_E}^t$. The LSTM unit presents two distinct states: i) the cell state $\boldsymbol{C}_{l_E}^t$ and ii) the LSTM output $\boldsymbol{H}_{l_E}^t$. The two states are related via:

- $\boldsymbol{C}_{l_E}^t = f_{l_E}^t \boldsymbol{C}_{l_E}^{t-1} + i_{l_E}^t \tanh\left(\boldsymbol{W}_{l_E}\boldsymbol{X}_{l_E}^t + \boldsymbol{U}_{l_E}\boldsymbol{H}_{l_E}^{t-1} + \boldsymbol{b}_{l_E}\right)$
- $\boldsymbol{H}_{l_E}^t = o_{l_E}^t \tanh\left(\boldsymbol{C}_{l_E}^t\right).$

$\boldsymbol{C}_{l_E}^{t-1}$ and $\boldsymbol{H}_{l_E}^{t-1}$ represent the previous cell and hidden states, respectively; $\boldsymbol{W}_{l_E}$ and $\boldsymbol{U}_{l_E}$ refer to the learning weights and $\varphi(\cdot)$ stands for the nonlinear activation function.

2) Latent Layer l_H: l_H enables a compressed representation of the input information. The latent layer holds the compact representation of data which is then concatenated with $\boldsymbol{X}_{l_E}$ and conveyed to the graph decoder.

3) Graph Decoder $D_{\mathcal{G}}$: The main aim of the graph decoder is to produce an output $\boldsymbol{X}^*$ that closely resembles the input $\boldsymbol{X}$. The reconstruction error η is measured as: $\eta = \|\boldsymbol{X}^* - \boldsymbol{X}\|^2$. Similar to the graph encoder, the outputs of the graph decoder are sequentially fed to the LSTM that processes time-evolving graph features. The LSTM updates its current hidden state $\boldsymbol{H}_{l_D}^t$ based on the current input from the graph decoder layer and the previous hidden state $\boldsymbol{H}_{l_D}^{t-1}$ seamlessly. 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. The decoder cell and hidden state are given by:

- $\boldsymbol{C}_{l_D}^t = f_{l_D}^t \boldsymbol{C}_{l_D}^{t-1} + i_{l_D}^t \tanh\left(\boldsymbol{W}_{l_D}^C \boldsymbol{X}_{l_D}^t + \boldsymbol{U}_{l_D}^C \boldsymbol{H}_{l_D}^{t-1} + \boldsymbol{b}_{l_D}^C\right)$.
- $\boldsymbol{H}_{l_D}^t = o_{l_D}^t \tanh\left(\boldsymbol{C}_{l_D}^t\right)$.

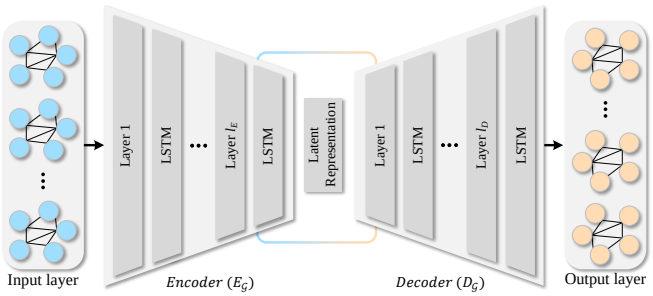

Fig. 2. Architecture of the proposed GAE.

V. Experimental Settings

This section describes the benchmark detectors, their hyperparameter optimization, and metrics for evaluating the model's performance and user satisfaction rate.

A. Benchmark Detectors

The benchmark detectors to reference the performance of the proposed approach include: i)ARIMA model, a shallow unsupervised learning method; ii) LSTM, a type of recurrent neural network (RNN) particularly designed for forecasting sequential data; iii) feedforward neural network (FNN), a supervised architecture that extracts features through stacked hidden layers of fully connected neurons; iv) CNN, which utilizes convolutional operations to dynamically learn features from data; and v) support vector machine (SVM), a supervised learning algorithm.

B. Hyperparameter Optimization

To optimize the detection performance, we utilize a sequential grid search algorithm to optimize the hyperparameters of both the proposed and benchmark detectors. The optimal hyperparameters, $\boldsymbol{\mathcal{H}}$ ={number of layer, number of neurons in each layer, dropout rate, optimizer, activation function, order of neighborhood} for CNN, FNN, LSTM, GCNN and GNN are (in order): $\boldsymbol{\mathcal{H}}_{\text{CNN}} = \{4, 32, 0.4, \text{Rmsprop}, 5, \text{Relu}\}$, $\boldsymbol{\mathcal{H}}_{\text{FNN}} = \{4, 32, 0, \text{Adam}, \text{N/A}, \text{Relu}\}$, $\boldsymbol{\mathcal{H}}_{\text{LSTM}} = \{3, 32, 0.2, \text{Adam}, \text{N/A}, \text{Relu}, \}$, and $\boldsymbol{\mathcal{H}}_{\text{GAN}} = \{6, 64, 0.2, \text{Adam}, 5, \text{Relu}\}$. For ARIMA model, we explored the search space from the set $\{0, 1, 2, 3\}$. Ultimately, we determined that the optimal values for the differencing degree and moving average were 1 and 0, respectively. For the SVM model, the optimal settings for the gamma, kernel, and regularization parameters were (in order): auto, sigmoid, and 1, respectively.

C. Metrics of performance evaluation

The performance metrics to evaluate the detection performance of the proposed FDIA detector include: 1) Detection rate, DR $= \frac{\text{TP}}{\text{TP+FN}}$, to assess the capacity to detect genuine attack samples; 2) False alarm rate, FAR $= \frac{\text{FP}}{\text{FP+TN}}$, to determine the frequency of non-malicious samples being mistakenly identified as threats; and 3) Accuracy, ACC $= \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}}$, to thoroughly evaluate the detector's efficacy in identifying both attack and normal samples. The variables: TN, TP, FN, and FP represent the count of true negatives, true positives, false negatives, and false positives, respectively.

D. Metric of User Experience

To evaluate the EV user charging experience, we employed the Ev users' charging satisfaction rate $\mathcal{S}$, defined as: $\mathcal{S} = \frac{P_{CS}}{N_{EV} \times P_{EV}}$. Here, P_{CS} indicates the available power at the charging stations. During attack situations, the true power reading of a CS, P_{CS} is altered with a false value, resulting in a higher number of unsatisfied users compared to the normal conditions.

VI. Experimental Results

This section presents the overall attack detection performance of the proposed model across different attack scenarios for the considered systems. A comparative performance analysis is carried out between the proposed approach and state-of-the-art benchmark detectors.

A. Performance Against Different Attack Scenarios

The performance of the proposed model against random bus attack and most vulnerable bus attack is depicted in Table II. The results reveal that the proposed model achieves higher performance against all the test cases. According to the simulation study, a slight enhancement of the detection performance is observed as the system size expands. This is attributed to the increase in the volume of data in larger systems, leading to improved performance. Specifically, when testing the proposed detectors on the 2000-bus system configurations, the model shows 0.9% to 2.5% performance improvement compared to the 30-bus system. From the table, we also infer that the model exhibits slightly less performance during random bus attacks. Among the benchmark detectors, CNN performs the closest to

TABLE I. Relative performance of the benchmark detectors.

Attack Strategy	System	Detector	Metric		
			DR	FAR	ACC
Random bus attack	2000-bus	**ARIMA**	59.41	53.98	58.33
		SVM	63.68	46.35	62.39
		FNN	70.02	37.59	68.60
		LSTM	75.09	30.15	73.54
		CNN	80.29	24.52	79.98
		GAE	99.11	8.20	98.74
	30-bus	**ARIMA**	58.03	55.63	57.22
		SVM	62.50	47.79	61.17
		FNN	69.00	39.11	67.43
		LSTM	75.01	31.54	71.65
		CNN	78.93	25.98	79.36
		GAE	98.83	8.32	97.94
Most vulnerable bus attack	2000-bus	**ARIMA**	56.62	54.84	55.67
		SVM	61.41	47.41	60.04
		FNN	68.11	39.61	66.08
		LSTM	72.83	31.89	71.03
		CNN	78.20	24.59	77.79
		GAE	97.02	8.83	96.79
	30-bus	**ARIMA**	54.33	55.94	53.37
		SVM	59.43	48.61	57.65
		FNN	66.05	39.93	64.2
		LSTM	70.67	31.97	69.21
		CNN	75.54	25.04	75.12
		GAE	96.48	8.90	96.31

the proposed detector while ARIMA performs the worst with an average of 35.44% accuracy. Overall, the proposed GAE-based detector shows a 15-30% improvement in detection performance over the test cases. Moreover, the average F1-score observed for the proposed model is 0.93 which indicates the high performance of the proposed model.

B. Impact of Attacks on User Satisfaction Rate

This section assesses the influence of cyber attacks on users' charging satisfaction rates. Table II portrays the user satisfaction rate for both random and vulnerable bus attack scenarios during attacks and subsequent to detection. During no-attack scenario with all allocated CSs, the user satisfaction rate is 89.36%. As interpreted from the table, during attack conditions the user satisfaction rate drops to 56.55-71.97%. During post-implementation, the satisfaction rate becomes 80.71-87.29% which signifies a 20-25% improvement in user satisfaction rate in comparison to the adversarial scenario. Such exceptional capability stems from its ability to generalize across various attack conditions.

TABLE II. $\mathcal{S}(\%)$ during attack and after detection using GAE.

		During attack		After detection	
System		**2000-bus**	**30-bus**	**2000-bus**	**30-bus**
RNA	**Additive**	71.97	70.57	87.29	86.20
	Deductive	70.63	68.91	84.92	84.33
	Combined	59.63	59.47	81.79	80.09
VNA	**Additive**	68.53	67.71	86.16	85.79
	Deductive	67.21	65.88	84.48	84.07
	Combined	56.55	55.29	80.71	78.81

VII. Conclusions

This paper presented a GAE-based FDIA detection framework specifically built for coupled power and transportation networks. Through extensive simulation studies, we evaluated the model's performance across various attack types and system topologies. The proposed detector exhibited high accuracy, reaching up to 98%, while substantially improving EV user satisfaction rates by 10-33%. Comparative performance analysis against benchmark detectors revealed a notable average improvement in detection rates for both situations: the case of random node attacks as well as the situation when the attacks are deployed on the most vulnerable nodes. The key aspect that ensured the success of the proposed detection framework is its ability to extract spatial-temporal features from the measurement data through the Chebyshev graph convolution filters. In addition, the proposed detector was trained on multiple system topologies that help to extend its generalization capabilities across multiple different networks. Future research directions may involve further optimization to reduce implementation complexity for real-time deployment and addressing dynamic changes and errors in network environments.

VIII. Acknowledgement

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

References

[1] J. C. Minx, W. F. Lamb, R. M. Andrew, J. G. Canadell, M. Crippa, N. Döbbeling, P. M. Forster, D. Guizzardi, J. Olivier, G. P. Peters *et al.*, "A comprehensive and synthetic dataset for global, regional, and national greenhouse gas emissions by sector 1970–2018 with an extension to 2019," *Earth System Science Data*, vol. 13, no. 11, pp. 5213–5252, 2021.

[2] Y. Sun, P. Zhao, L. Wang, and S. M. Malik, "Spatial and temporal modelling of coupled power and transportation systems: A comprehensive review," *Energy Conversion and Economics*, vol. 2, no. 2, pp. 55–66, 2021.

[3] X. Yin, Y. Zhu, and J. Hu, "A subgrid-oriented privacy-preserving microservice framework based on deep neural network for false data injection attack detection in smart grids," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 1957–1967, 2021.

[4] H. Long, Z. Wu, C. Fang, W. Gu, X. Wei, and H. Zhan, "Cyber-attack detection strategy based on distribution system state estimation," *Journal of Modern Power Systems and Clean Energy*, vol. 8, no. 4, pp. 669–678, 2020.

[5] P. Zhuang, R. Deng, and H. Liang, "False data injection attacks against state estimation in multiphase and unbalanced smart distribution systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6000–6013, 2019.

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

[7] A. Meng, H. Wang, S. Aziz, J. Peng, and H. Jiang, "Kalman filtering based interval state estimation for attack detection," *Energy Procedia*, vol. 158, pp. 6589–6594, 2019.

[8] 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. 31 762–31 773, 2019.

[9] Y. Zhang, J. Wang, and B. Chen, "Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 623–634, 2020.

[10] Y. Wang, Z. Zhang, J. Ma, and Q. Jin, "Kfrnn: An effective false data injection attack detection in smart grid based on kalman filter and recurrent neural network," *IEEE Internet of Things Journal*, vol. 9, no. 9, pp. 6893–6904, 2021.

[11] G. Zhang, J. Li, O. Bamisile, D. Cai, W. Hu, and Q. Huang, "Spatio-temporal correlation-based false data injection attack detection using deep convolutional neural network," *IEEE Transactions on Smart Grid*, vol. 13, no. 1, pp. 750–761, 2021.

[12] T. Ishizaki, A. Chakrabortty, and J.-I. Imura, "Graph-theoretic analysis of power systems," *Proceedings of the IEEE*, vol. 106, no. 5, pp. 931–952, 2018.

[13] 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 Transactions on Smart Grid*, vol. 13, no. 1, pp. 807–819, 2021.

[14] 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 & Security*, vol. 124, p. 103016, 2023.

[15] A. Takiddin, M. Ismail, U. Zafar, and E. Serpedin, "Robust electricity theft detection against data poisoning attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 2675–2684, 2020.

[16] J. B. Hansen, S. N. Anfinsen, and F. M. Bianchi, "Power flow balancing with decentralized graph neural networks," *IEEE Transactions on Power Systems*, 2022.

[17] G. J. Correa and J. M. Yusta, "Grid vulnerability analysis based on scale-free graphs versus power flow models," *Electric Power Systems Research*, vol. 101, pp. 71–79, 2013.

[18] R. Kinney, P. Crucitti, R. Albert, and V. Latora, "Modeling cascading failures in the north american power grid," *The European Physical Journal B-Condensed Matter and Complex Systems*, vol. 46, no. 1, pp. 101–107, 2005.

[19] F. Jamour, S. Skiadopoulos, and P. Kalnis, "Parallel algorithm for incremental betweenness centrality on large graphs," *IEEE Transactions on Parallel and Distributed Systems*, vol. 29, no. 3, pp. 659–672, 2017.

[20] S. Chanda and A. K. Srivastava, "Defining and enabling resiliency of electric distribution systems with multiple microgrids," *IEEE Transactions on Smart Grid*, vol. 7, no. 6, pp. 2859–2868, 2016.