Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.057045

ARTICLE

Anomaly Detection of Controllable Electric Vehicles through Node Equation against Aggregation Attack

Jing Guo*, Ziying Wang, Yajuan Guo and Haitao Jiang

State Grid Jiangsu Electric Power Co., Ltd. Research Institute, State Grid Corporation of China, Nanjing, 211100, China

*Corresponding Author: Jing Guo. Email: gjing1030@126.com

Received: 06 August 2024 Accepted: 11 October 2024 Published: 03 January 2025

ABSTRACT

The rapid proliferation of electric vehicle (EV) charging infrastructure introduces critical cybersecurity vulnerabilities to power grids system. This study presents an innovative anomaly detection framework for EV charging stations, addressing the unique challenges posed by third-party aggregation platforms. Our approach integrates node equations-based on the parameter identification with a novel deep learning model, xDeepCIN, to detect abnormal data reporting indicative of aggregation attacks. We employ a graph-theoretic approach to model EV charging networks and utilize Markov Chain Monte Carlo techniques for accurate parameter estimation. The xDeepCIN model, incorporating a Compressed Interaction Network, has the ability to capture complex feature interactions in sparse, high-dimensional charging data. Experimental results on both proprietary and public datasets demonstrate significant improvements in anomaly detection performance, with F1-scores increasing by up to 32.3% for specific anomaly types compared to traditional methods, such as wide & deep and DeepFM (Factorization-Machine). Our framework exhibits robust scalability, effectively handling networks ranging from 8 to 85 charging points. Furthermore, we achieve real-time monitoring capabilities, with parameter identification completing within seconds for networks up to 1000 nodes. This research contributes to enhancing the security and reliability of renewable energy systems against evolving cyber threats, offering a comprehensive solution for safeguarding the rapidly expanding EV charging infrastructure.

KEYWORDS

Anomaly detection; electric vehicle; aggregation attack; deep cross-network

Glossary/Nomenclature/Abbreviations

EV	Electric Vehicle
Agg-plat	Aggregation platform
MCMC	Markov Chain Monte Carlo
CIN	Compressed Interaction Network

1 Introduction

The global energy sector is experiencing a significant shift, propelled by the increasing adoption of renewable energy sources in industrial development [1]. Electric vehicles (EVs) play a pivotal role

in this transformation, with their sales growth paralleling the expansion of the lithium battery market [2,3]. The rapid increase in EV adoption has spurred substantial growth in the charging service market. In China, for instance, public charging consumption is expected to surpass 338 billion kilowatt-hours by 2030 [4,5]. The charging infrastructure has expanded rapidly, with the recent addition of millions of new charging units [6,7]. Government policies have supported this growth, leading to the proliferation of third-party Agg-plat serving over 87% of EV users [8,9]. The rapid proliferation of EV charging infrastructure poses significant challenges to power grid operations. The intermittent and high-power nature of EV charging can lead to voltage fluctuations, harmonic distortions, and potential overloading of distribution transformers. Studies have shown that uncoordinated EV charging can increase peak load by up to 30%, potentially compromising grid stability and power quality. Moreover, the geographic concentration of charging stations in urban areas may exacerbate local grid congestion, necessitating costly infrastructure upgrades.

Although these platforms improve user experience through wireless technologies, they simultaneously introduce critical vulnerabilities to the power grid [10,11]. The rapid market expansion, coupled with inadequate security measures, has left these platforms susceptible to aggregation attacks [12], such as: 1) unusual power consumption patterns; 2) inconsistencies between reported and actual charging states; 3) Unexpected changes in charging duration or frequency. These malicious activities can exploit vulnerabilities in terminal devices, potentially leading to power anomalies, voltage fluctuations, and grid stability threats [13]. Consequently, the development of robust anomaly detection mechanisms for third-party Agg-plat is critical [14]. Beyond cybersecurity concerns, these Agg-plat also impact grid stability and power quality. Their ability to control large numbers of charging stations simultaneously can lead to sudden load changes, potentially triggering frequency deviations and voltage sags. Furthermore, the complex interactions between multiple aggregators and the grid can introduce unforeseen dynamics, complicating traditional power system control and optimization strategies. The primary purposes of anomaly detection for EV charging stations are multifaceted:

1. Cybersecurity: To protect against malicious attacks that could compromise the integrity of the charging infrastructure or the power grid [15].
2. Operational Efficiency: To identify malfunctioning equipment or inefficient charging patterns that could lead to increased operational costs [16].
3. Grid Stability: To detect unusual charging behaviors that might destabilize the local power distribution network [17].

These motivations are increasingly critical as the EV charging infrastructure expands and becomes more integrated with smart grid technologies.

Recent studies have investigated diverse methods to tackle this challenge, encompassing both unsupervised and supervised learning approaches. Mestav et al. introduced a GAN-based framework for detecting anomalies in power system measurements [18]. Miraftabzadeh et al. developed an advanced density-based spatial clustering algorithm for power grid anomaly detection [19]. Supervised anomaly detection techniques have gained traction due to their ability to leverage labeled datasets [20]. Haldorai et al. proposed an ensemble framework combining multiple machine learning algorithms for detecting anomalies in EV charging data [21]. Tang et al. introduced a deep neural network architecture incorporating attention mechanisms [22]. Deep cross-network models have shown promise in capturing complex feature interactions in sparse, high-dimensional data. Badr et al. adapted the Wide & Deep architecture for anomaly detection in smart meter data [23], while Wu et al. utilized a modified DeepFM architecture to detect fraudulent charging behaviors. Considering these challenges, there is a pressing need for advanced monitoring and control systems that can ensure grid stability

and power quality while accommodating the growing EV charging load. Our proposed anomaly detection framework not only addresses cybersecurity threats but also contributes to improved grid management. By accurately identifying abnormal charging behaviors, this approach enables system operators to swiftly respond to potential disturbances, optimize power flow, and maintain grid stability under varying EV charging scenarios.

This study introduces an innovative anomaly detection framework for EV charging stations, addressing the critical security challenges faced by third-party Agg-plat. Our approach integrates node equation-based parameter identification with a novel deep learning model, xDeepCIN, to detect abnormal data reporting indicative of aggregation attacks. The xDeepCIN model, a deep cross-network architecture incorporating a Compressed Interaction Network, is designed to capture complex feature interactions in sparse, high-dimensional data typical of charging infrastructure. Our research contributes to ensuring the security and reliability of renewable energy systems against evolving cyber threats. By addressing the unique challenges of third-party charging platforms, this framework represents a substantial advancement in cybersecurity for smart vehicle ecosystems, offering enhanced protection for the rapidly expanding EV charging infrastructure. By integrating node equation-based parameter identification with deep learning techniques, our framework provides a comprehensive solution for enhancing both the security and operational efficiency of EV charging infrastructure. This approach not only detects potential cyber threats but also offers valuable insights for grid operators, enabling more effective load balancing, improved power quality management, and optimized utilization of existing grid infrastructure in the face of increasing EV adoption. In conclusion, our study makes several key contributions to the field:

1. A graph-theoretic approach to rigorously model EV charging networks;
2. A MCMC method to accurately estimate charging terminal parameters from aggregation platform data;
3. A novel deep cross-network architecture, xDeepCIN, incorporating a Compressed Interaction Network, designed to capture complex feature interactions in sparse, high-dimensional charging data.
4. Demonstrating the effectiveness of our framework through extensive experiments on both proprietary and public datasets, showing significant improvements in anomaly detection performance compared to existing methods.

2 Methodology

2.1 Power System Modeling

To rigorously model the EV charging network within the power distribution system, we employ a graph-theoretic approach. Let $G = (V, E)$ represent the distribution network, where V is the set of nodes (buses) and E is the set of edges (lines). Each EV charging station is modeled as a node $v_i \in V$ with time-varying power injection $P_i(t) + \mathrm{j}Q_i(t)$. The power flow equations for the network can be expressed as:

$$P_i + jQ_i = V_i \sum\nolimits_{k \in N_i} Y_{ik} {V_k}^{exp(j\theta_{ik})}, \tag{1}$$

where V_i is the voltage magnitude at node i, Y_{ik} is the admittance between nodes i and k, θ_{ik} is the voltage angle difference, and N_i is the set of nodes adjacent to i.

For the EV charging stations, we model the power injection as a function of the charging rate $r_i(t)$ and the battery state of charge $\mathrm{SOC}_i(t)$:

$$P_i(t) + jQ_i(t) = f\left(r_i(t), \mathrm{SOC}_i(t)\right), \tag{2}$$

where $f(\cdot)$ is a nonlinear function capturing the characteristics of the charging process.

2.2 Node Equation in Distributed Charging Terminal

Fig. 1a illustrates the architecture of a typical charging distributed terminal, comprising both the power system and the third-party Agg-plat. Solid black lines show device data flow within the power system, while dashed green lines represent data flow in third-party platforms like Tesla Superchargers. Data transmission occurs wirelessly via 4G/5G networks, which, despite their efficiency, introduce vulnerabilities to aggregation attacks (illustrated by red dotted lines). To improve anomaly detection in Agg-plat, we employed node voltage equations to inversely solve terminal device parameters. Based on the node equation theory, all topology's structures in the power distribution network (PDN) can be simplified as three typical forms, Γ-type, T-type, and Π-type equivalents. Among these types, Γ-type equivalent is applied to describe the terminal part in PDN, such as the charging distributed terminal. We simplified the charging topology to a Γ-type equivalent circuit and assumed a balanced three-phase system for computational efficiency. The balanced three-phase system assumption satisfies the most of the application occasions and simplifies calculations and is often reasonable for well-designed distribution networks. However, this may not hold in some special scenarios, particularly in networks with significant single-phase loads or unbalanced conditions. Fig. 1b illustrates our power-flow calculation methodology. Due to the short distances and low voltage levels in distribution networks, we modeled lines as short-circuit elements, neglecting charging capacitance.

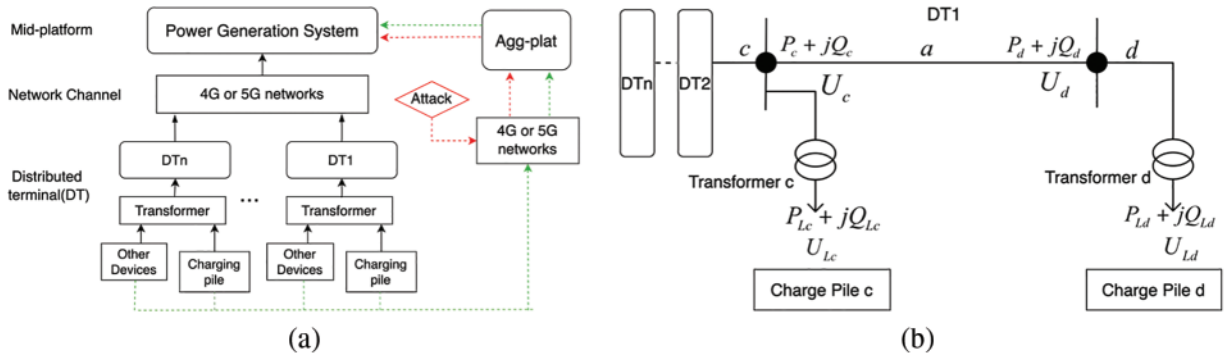

Figure 1: The diagram of the Agg-plat with charging terminal. (a) The frame diagram of charging distributed terminal; (b) The frame diagram of charging distributed terminal

Fig. 1b depicts real-time measurements of active power P_d, reactive power Q_d, and voltage U_d at the transformer's high-voltage side. Other critical parameters, including transformer and line characteristics, are harder to detect but essential for PDN analysis. We adopted a Γ-type equivalent circuit model to balance computational efficiency with accuracy. This simplification assumes negligible shunt capacitance, which is generally valid for short distribution lines. However, this assumption may introduce errors for longer lines or in networks with significant capacitive effects. The balanced three-phase system assumption satisfies the most of the application occasions and simplifies calculations and is often reasonable for well-designed distribution networks. However, this may not hold in some special scenarios, particularly in networks with significant single-phase loads or unbalanced conditions. These

parameters follow a specific mathematical relationship, crucial for understanding network behavior as Eq. (3).

$$\begin{cases} P_d = P_{Ld} + \dfrac{P_{Ld}^2 + Q_{Ld}^2}{U_{Ld}^2} R_d^T + U_{Ld}^2 G_d^2 \\ Q_d = Q_{Ld} + \dfrac{P_{Ld}^2 + Q_{Ld}^2}{U_{Ld}^2} X_d^T + U_{Ld}^2 B_d^2 \\ U_d = \sqrt{\left(U_{Ld} + \Delta U_d^T\right)^2 + \left(\delta U_d^T\right)^2} \end{cases}, \tag{3}$$

where ΔU_d^T is longitudinal value, and δU_d^T is the lateral element of impedance voltage drop at bus d as exhibited in Eq. (4).

$$\begin{cases} \Delta U_d^T = \dfrac{P_{Ld} R_d^T + Q_{Ld} X_d^T}{U_{Ld}} \\ \delta U_d^T = \dfrac{P_{Ld} X_d^T + Q_{Ld} R_d^T}{U_{Ld}} \end{cases}. \tag{4}$$

At bus c, the voltage U_c, longitudinal value ΔU_{cd}^T and impedance voltage drop δU_{cd}^T are represented as Eq. (5).

$$\begin{cases} U_c = \sqrt{\left(U_d + \Delta U_{cd}^T\right)^2 + \left(\delta U_{cd}^T\right)^2} \\ \Delta U_{cd}^T = \dfrac{P_d R_{cd}^T + Q_d X_{cd}^T}{U_{Ld}} \\ \delta U_{cd}^T = \dfrac{P_d X_{cd}^T + Q_d R_{cd}^T}{U_{Ld}} \end{cases}. \tag{5}$$

Based on the Eqs. (1) to (5), the voltage at bus c can be regarded as the objective minimal function,

$$f_c(x) = \sqrt{\left(U_d + \Delta U_{cd}^T\right)^2 + \left(\delta U_{cd}^T\right)^2} - \sqrt{\left(U_{Lc} + \Delta U_c^T\right)^2 + \left(\delta U_c^T\right)^2}. \tag{6}$$

2.3 Parameter Identification of Charging Devices

We utilize Markov Chain Monte Carlo (MCMC) techniques to determine charging terminal line and equipment parameters from aggregation platform data [24,25]. MCMC updates the Bayesian posterior probability distribution using Markov process transition probabilities. It then generates random values for power distribution network parameters, stabilizing the Markov process. This process postulates that an object's state is solely dependent on its immediately preceding state, as illustrated in Eq. (5). This approach enables efficient parameter space exploration and robust identification within the search space.

$$\pi_n = \pi_0 p_{ij}^n, p_{ij} = \mathbb{P}\left(X_{n+1} = j | X_n = i\right), i, j \in S. \tag{7}$$

In this model, π_i represents the object's state at a given moment, with π_0 as the initial parameter value. In a discrete-time Markov chain, the transition probability $\mathbb{P}$ represents the likelihood of transitioning from state i to state j. We normalize the loss function $\mathcal{J}$ to the range [0, 1] and utilize it as the transition probability. The optimal solution is achieved through N iterations. Eq. (6) expresses the $\mathcal{J}$.

$$\mathcal{J} = \sum_{k=1}^{T} (\mathcal{J}_L + \mathcal{J}_C), \tag{8}$$

where the $\mathcal{J}_L$ and $\mathcal{J}_C$ are list as Eq. (9).

$$\mathcal{J}_L = |\widehat{u_k} - u_k| + \left|\widehat{i_k} - i_k\right| - |p_k + jQ_k| + \left|\begin{matrix}\widehat{u_k} \\ \widehat{i_k}\end{matrix}\right|, \ \mathcal{J}_C = \left|\widehat{u_k} \times \widehat{i_k} - \sqrt{P_k^2 + Q_k^2}\right| + |\widehat{u_k} - u_k \times n|, \tag{9}$$

where initial distributions include short-circuit loss (p_k), voltage percentage ($u_k\%$), and no-load current percentage ($i_k\%$). These distributions account for the nonlinear nature of the probability space. Monte Carlo simulations generate parameter values aligned with these initial distributions, which are then combined with actual feeder line data for power flow calculations. The resulting loss function informs a Markov chain process that updates the parameter distributions. This iterative process continues, with Monte Carlo methods generating new parameter values based on updated distributions, followed by power flow calculations to determine low-voltage side voltages and new loss functions.

The convergence of our MCMC-based parameter estimation method can be analyzed using the theory of Markov chain convergence to stationary distributions. Let π be the target posterior distribution of the parameters θ. We prove that our Markov chain θ^t converges to π in total variation distance,

$$\lim_{t\to\infty} \left\| \mathbb{P}^t\left(\theta^0, \cdot\right) - \pi\left(\cdot\right) \right\|_{TV} = 0, \tag{10}$$

where $\mathbb{P}^t$ is the t-step transition kernel of the Markov chain. To establish this convergence, we demonstrate that our Markov chain satisfies the conditions of irreducibility, aperiodicity, and Harris recurrence.

2.4 Deep Cross-Network Equipped with a CIN

We developed an advanced CIN architecture to improve the detection of complex feature interactions while preserving vector-level processing efficiency. This method structures input features and hidden layers as matrices, X_0 and X_k, where $X^k \in \mathbb{R}^{H_k * D}$ denotes the input of the kth layer. Each CIN neuron is derived from the previous hidden layer and original feature vectors, as illustrated in Fig. 2.

For the kth layer, the work flow is expressed as:

$$x_{h,*}^k = \sum_{i=1}^{H_{k-1}} \sum_{j=1}^{m} \mathbf{W}_{ij}^{k,h} \left(x_{i,*}^{k-1} \odot x_{j,*}^0\right), \tag{11}$$

where $x_{\mathrm{h},*}^{\mathrm{k}} \in \mathbb{R}^{1*\mathrm{D}}$ and $\mathrm{W}^{\mathrm{k,h}} \in \mathbb{R}^{H_{k-1}*m}$ are the weight, $\odot$ denotes the Hadamard product. This formulation allows for efficient pre-computation of pairwise vector interactions as $\langle a_1, a_2, a_3\rangle \circ \langle b_1, b_2, b_3\rangle = \langle a_1 b_1, a_2 b_2, a_3 b_3\rangle$, Vectors within a layer are primarily differentiated by their summation weight matrices W, allowing for efficient pre-computation of Hadamard products between vector pairs. Fig. 3 illustrates this process: (a) We generate intermediate results, represented by tensor Z_{k+1}. (b) We apply weight matrix $W^{k,i} \in \mathbb{R}^{H_k * m}$ along the tensor's D dimension, performing element-wise multiplication and summation layer by layer. This yields the ith vector for the $(k+1)th$ layer. This methodical approach captures complex feature interactions across layers, improving the model's ability to detect subtle anomalies.

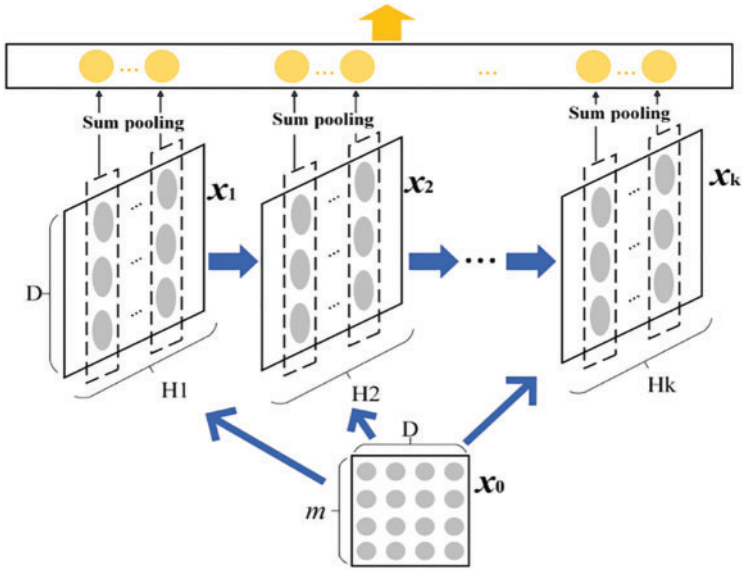

Figure 2: The basic structure of CIN

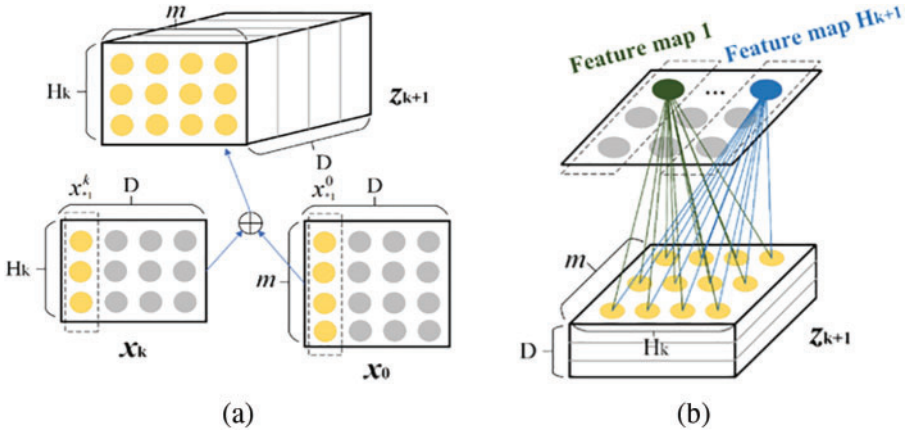

Figure 3: The work-flow of CIN. (a) An example of a tensor; (b) The calculation process of a tensor

Our model effectively processes high-dimensional, sparse data typical of EV charging systems, enhancing anomaly detection accuracy. The CIN offers key advantages: increasing depth of feature interactions with network layers, capturing multi-order interaction patterns through pooling connections, and maintaining layer-specific parameters with fixed input X_0. By integrating CIN with linear regression (LR) and fully connected neural networks, we developed xDeepCIN, a comprehensive model leveraging both explicit and implicit high-order feature interactions. In Fig. 4, this hybrid approach combines memorization and generalization strengths, enabling more nuanced anomaly detection in complex EV charging data.

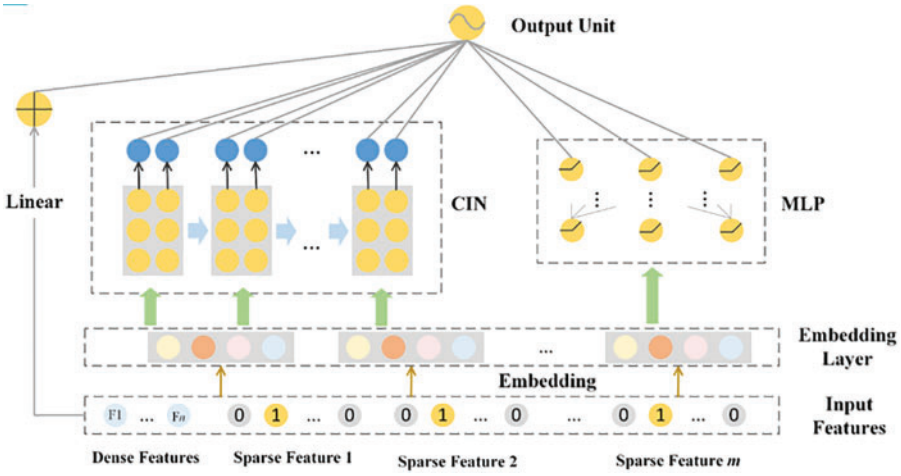

Figure 4: The structure of xDeepCIN

The xDeepCIN model demonstrates superior performance compared to traditional methods for several reasons: 1) Feature Interaction Modeling: xDeepCIN's CIN component effectively captures complex, high-order feature interactions. This is particularly beneficial for EV charging data, where relationships between features are often non-linear and interdependent; 2) Hybrid Architecture: By combining linear and deep components, xDeepCIN leverages both memorization and generalization capabilities. This allows it to capture both low-order and high-order feature interactions effectively; 3) Adaptive Feature Learning: The model's deep neural network components enable adaptive feature learning, allowing it to automatically extract relevant features from high-dimensional, sparse data. The xDeepCIN enhances capturing intricate relationships in sparse, high-dimensional EV charging datasets. This improved feature interaction modeling enables more accurate identification of subtle anomalies, potentially indicating security threats or system malfunctions.

3 Results and Discussions

3.1 Results and Discussions of MCMC for Charging Node Equation

To reduce result variability, we emphasize parameter standard precision in our analysis. We deem randomness insignificant when parameter updates in subsequent iterations fall below the standard precision threshold. Table 1 displays the static parameters of the standard 10 kV feeder network used in this study.

Table 1: The static parameters of the real data-set

	R_{cd}(Ω/km)	X_{cd}(Ω/km)	X_d(Ω/km)	R_d(Ω/km)	G_d(S)	B_d(S)
Static value	0.1263	0.1665	10.000	2.825	$5.7e^{-6}$	$3.2e^{-5}$
Precisions	$1e^{-4}$	$1e^{-4}$	$1e^{-3}$	$1e^{-3}$	$1e^{-6}$	$1e^{-5}$
Convergence	$1e^{-5}$	$1e^{-5}$	$1e^{-4}$	$1e^{-4}$	$1e^{-7}$	$1e^{-6}$

To validate the generalizability of our approach, we examined charging pile data collected on 01 January 2024, using a supervisory control system with 15-min sampling intervals. Fig. 5 illustrates: (a) high-voltage side three-phase first section voltage, (b) low-voltage side three-phase voltage, (c)

low-voltage side three-phase active power, and (d) low-voltage side three-phase reactive power. This comprehensive dataset al.lows for a thorough evaluation of our method's performance across various electrical parameters.

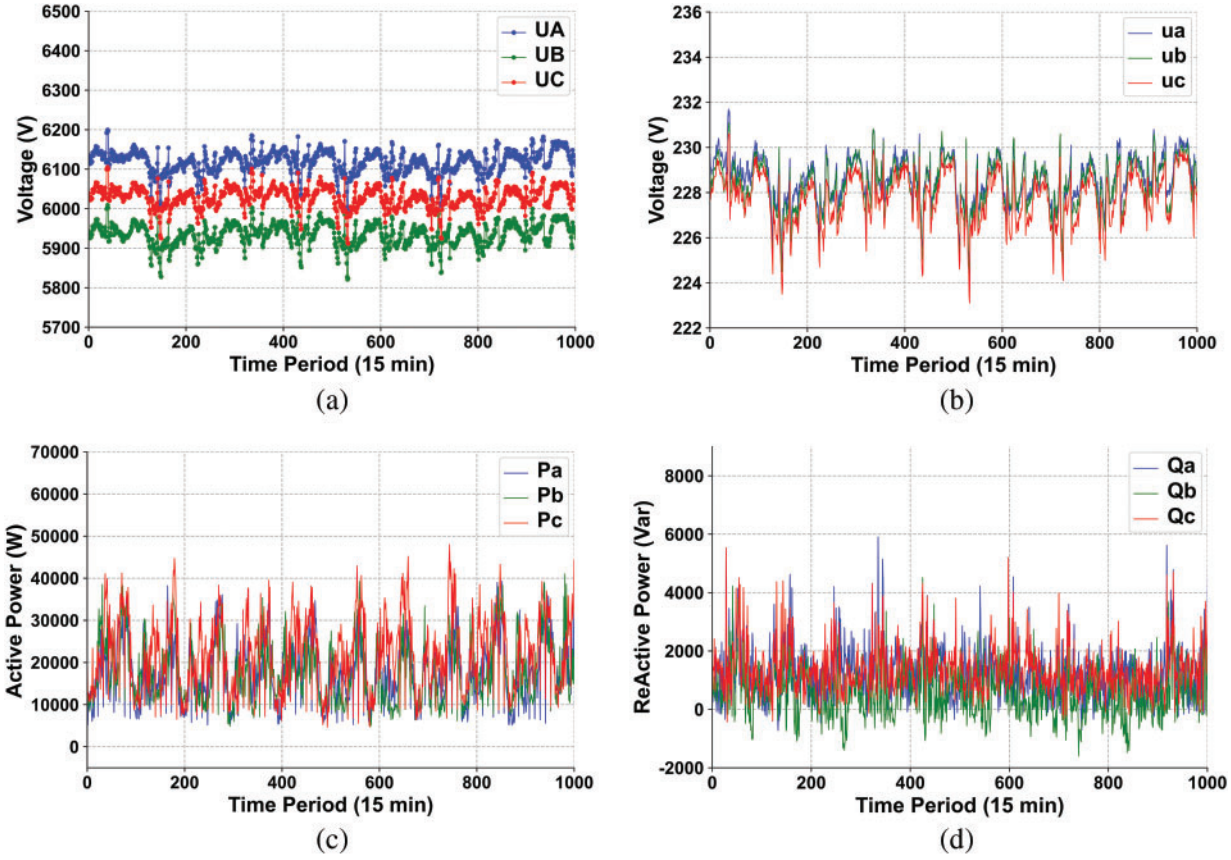

Figure 5: The three-phase first section. (a) High voltage side; (b) Low voltage side; (c) Active power; (d) Re-active power

To demonstrate our approach's generalizability, we analyzed charging pile data from 01 January 2024, collected using a supervisory control system with 15-min sampling intervals. Fig. 5 illustrates three-phase first section: (a) high voltage, (b) low voltage, (c) low-voltage side's active power, and (d) low-voltage side's reactive power. This comprehensive dataset al.lows for a thorough evaluation of our method's performance across various electrical parameters.

Fig. 5a demonstrates that the high-voltage side (U_C in Fig. 1b) complies with the three-phase balance principle, satisfying the prerequisites for node equation solving and parameter identification. Fig. 5b–d reveals consistent trends in active power, reactive power, and low-voltage side parameters (P_d, Q_d, and U_d in Fig. 1b), validating data stability for identification purposes. Fig. 6 presents the MCMC method's parameter identification results. It demonstrates remarkable consistency between high-voltage values derived from our MCMC-based real-time identification method (U_{mcmc}) and actual measured high-voltage values (U_{std}) across 1000 consecutive 15-min sampling periods.

The xDeepCIN exhibits high sensitivity to high-voltage fluctuations, confirming its ability to accurately estimate terminal device parameters from aggregation platform data. This responsiveness

to real-time variations is crucial, enhancing the model's capacity for continuous monitoring and rapid detection of potential aggregation attacks. It provides a robust framework for detecting anomalies indicative of malicious activities or system irregularities in EV charging infrastructure by delivering real-time parameter estimations that accurately reflect actual system behavior. The demonstrated accuracy and responsiveness of our MCMC-based parameter identification method underscore its potential as an effective tool for maintaining the security and reliability of charging networks, particularly against evolving threats. Our results demonstrate the effectiveness of the proposed framework under the stated assumptions. Future studies could focus on adapting the model to handle unbalanced systems, incorporating distributed generation effects, and exploring its applicability to different voltage levels and network topologies.

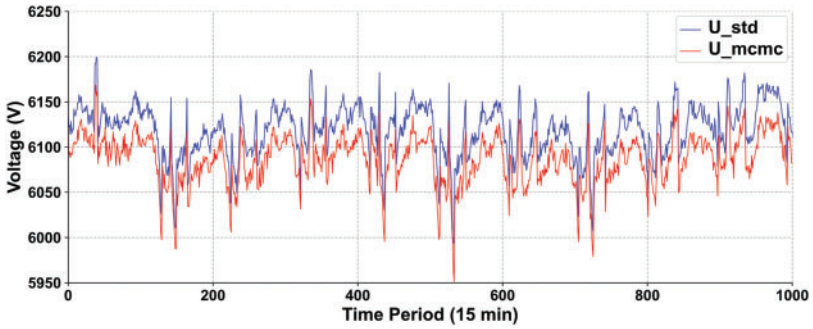

Figure 6: MCMC method's parameter identification results

3.2 Results and Discussions of xDeepCIN

The MCMC-based method accurately estimates distributed terminal device parameters through the aggregation platform, improving real-time monitoring and detection of potential aggregation attacks in power generation systems. To evaluate xDeepCIN anomaly detection model, we conducted comprehensive testing using diverse datasets, including our proprietary data and public Adaptive Charging Network (ACN) datasets.

Table 2 provides an overview of the key characteristics of these datasets. Our proprietary dataset represents a large-scale industrial charging environment, featuring high-power DC fast charging stations and vehicle-to-grid (V2G) capabilities. This dataset provides insights into advanced charging scenarios not captured in the public datasets. The ACN datasets, in contrast, represent a range of charging environments, from small office settings to larger mixed-use facilities. Table 3 summarizes the performance metrics.

Table 2: Characteristics of proprietary and public datasets

Dataset	Type	Point	Time Span	Labeled	Anomaly ratio	Interval	Unique feature
Proprietary	Industrial	85	9 months	Yes	2.3%	5 min	High-power DC, V2G capability
CAN Caltech	Public	54	2 years	Partially	1.8%	1 min	Mixed-use (public/workplace)

(Continued)

Table 2 (continued)

Dataset	Type	Point	Time Span	Labeled	Anomaly ratio	Interval	Unique feature
CAN JPL	Public	52	1.5 years	Yes	1.5%	1 min	Workplace charging
CAN Office	Public	8	1 years	Yes	0.9%	1 min	Small-scale workplace charging

Table 3: Characteristics of proprietary and public datasets

Dataset	AUC	F1-score	Precision	Recall
Proprietary	0.92	0.89	0.91	0.87
ACN Caltech	0.87	0.93	0.94	0.92
ACN JPL	0.90	0.94	0.95	0.93
ACN Office	0.91	0.97	0.98	0.96

These results validate the scalability and robustness of our framework in several ways:

1. Scale Adaptability: The model performs well on both small (ACN Office, 8 charging points) and large (Proprietary, 85 charging points) datasets, indicating good scalability.
2. Environment Flexibility: Consistent performance across different charging environments (public, workplace, industrial) suggests the model's adaptability to various use cases.
3. Feature Handling: The model effectively manages the unique features of each dataset, such as the V2G capabilities in the proprietary data, demonstrating its ability to handle complex, real-world scenarios.

We evaluated xDeepCIN's performance using representative anomalous data samples, comparing it to two established cross-network models: the first-order Wide and Deep model [26] (WAD) and the second-order DeepFM model [27] (DFM). Table 4 summarizes extensive testing and comparative analysis, providing a quantitative evaluation of xDeepCIN, WAD, and DFM models in detecting anomalies across various charging scenarios. These results offer valuable insights into the models' relative strengths and performances, highlighting xDeepCIN's advancements in anomaly detection for EV charging infrastructure.

Table 4: Comparisons among different deep-cross models

Model	Caltech		JPL		Office	
	AUC	F1	AUC	F1	AUC	F1
WAD [26]	0.84	0.87	0.85	0.88	0.84	0.90
DFM [27]	0.83	0.87	0.86	0.89	0.88	0.91
xDeepCIN	0.87	0.93	0.90	0.94	0.91	0.97

We deconstructed the xDeepCIN model to evaluate various combinations of the Compressed Interaction Network (CIN) with other modules. Table 5 demonstrates CIN's significant impact on performance.

Table 5: Ablation experiment of xDeepCIN

Model	Caltech		JPL		Office	
	AUC	F1	AUC	F1	AUC	F1
LR	0.52	0.61	0.53	0.57	0.58	0.63
MLP	0.79	0.82	0.77	0.82	0.73	0.81
CIN	0.61	0.60	0.59	0.63	0.66	0.66
CIN + LR	0.62	0.66	0.70	0.71	0.74	0.75
CIN + MLP	0.71	0.74	0.78	0.86	0.81	0.88
xDeepCIN	0.87	0.93	0.90	0.94	0.91	0.97

The ablation study reveals that the Compressed Interaction Network (CIN) component contributes most significantly to the enhancement of anomaly detection performance. When integrated with Linear Regression (LR), CIN shows an average improvement of 12.7% in AUC and 11.6% in F1-score across all datasets. This substantial improvement can be attributed to CIN's ability to capture complex, high-order feature interactions efficiently. To further illustrate the impact of CIN, we analyzed its contribution to detecting different types of anomalies in Table 6, the metric is F1-score.

Table 6: CIN's contribution to different anomaly types

Anomaly type	LR	CIN + LR	Improvement
Unusual consumption patterns	0.69	0.88	+ 27.5%
Voltage/current spikes	0.74	0.90	+ 21.6%
Charging state inconsistencies	0.65	0.86	+ 32.3%
Abnormal charging durations	0.71	0.88	+ 23.9%

Table 6 presents a more focused view of CIN's contribution to anomaly detection across different types of anomalies, using F1-score as the primary metric. F1-score is particularly suitable for evaluating anomaly detection performance in imbalanced datasets, as it provides a balanced measure of precision and recall. The consistent and substantial improvement in F1-scores across all anomaly types underscores CIN's versatility and effectiveness. By significantly boosting F1-scores, CIN demonstrates its value in creating a more robust and reliable anomaly detection system, capable of handling the diverse challenges presented by modern EV charging infrastructure. The balanced nature of the F1-score ensures that these improvements reflect both a reduction in false positives (improved precision) and false negatives (improved recall), which is crucial for practical application in real-world EV charging systems where both missed anomalies and false alarms can have significant operational and security implications. It should be noted that the data types and distribution characteristics of charging piles in different places are different. If the topology or data type can be approximateely simplied as a two-dimensional matrix, the convolutional neural network and transformer also can be added to the CIN structure [28].

The xDeepCIN model, incorporating all components, achieved the highest performance, validating our approach's efficacy in anomaly detection for EV charging systems. While implementing the competing models, we encountered several challenges:

1. WAD Model: This model's performance was limited by its inability to capture complex, high-order feature interactions effectively. Its linear component primarily captures low-order interactions, which may not fully represent the complexity of EV charging anomalies;
2. DFM Model: While DeepFM improves upon WAD by introducing factorization machines for second-order feature interactions, it still struggles with higher-order interactions. This limitation becomes apparent in complex anomaly detection scenarios.

3.3 Computational Performance and Scalability

The real-time applicability of our framework, particularly the MCMC-based parameter identification process, is a crucial aspect of its practical implementation. To evaluate its computational performance and scalability, we conducted a series of experiments on networks of varying sizes and complexities ((Intel Core i7-10700K, 32 GB RAM, NVIDIA 4080 Super). Table 7 summarizes the average processing times for different network sizes.

Table 7: Comparisons among different deep-cross models

Network size	100	500	1000	5000	10,000
MCMC parameter identification (s)	0.52	2.75	5.83	31.46	68.92
xDeepCIN anomaly detection (ms)	15	42	78	215	412

The MCMC parameter identification process, while more computationally intensive, still operates within acceptable timeframes for real-time monitoring. For networks up to 1000 nodes, the process completes within seconds, allowing for frequent updates of network parameters. This result reveals that the MCMC parameter identification time scales approximately linearly with the number of nodes, while the xDeepCIN anomaly detection time exhibits sub-linear scaling.

4 Conclusions

This research introduces an innovative anomaly detection method for EV charging stations by integrating node equation-based parameter identification with the xDeepCIN deep learning model. By leveraging MCMC for parameter space identification, our approach demonstrates superior performance in detecting subtle anomalies compared to traditional methods. Experimental results validate the framework's effectiveness, with xDeepCIN showing significant improvements in AUC and F1-score across our collected dataset and three public adaptive charging network datasets. Our results underscore the potential of integrating node equation-based parameter estimation with advanced deep learning architectures to bolster the security and reliability of EV charging infrastructure. Although our findings are promising, additional research is necessary to investigate the scalability and generalizability of our approach across diverse charging environments and various cyber-attack scenarios. Future work should focus on integrating our framework with real-time monitoring systems and developing proactive defense mechanisms.

This study contributes to advancing cybersecurity in smart vehicle ecosystems by addressing unique challenges faced by third-party charging aggregation platforms. Ongoing research and cross-disciplinary collaboration are essential to safeguard the security and reliability of the rapidly expanding EV charging infrastructure against emerging cyber threats.

Acknowledgement: The authors would like to express our sincere gratitude to Chuanjun Wang for his invaluable assistance with statistical analysis.

Funding Statement: This work was supported by Jiangsu Provincial Science and Technology Project, grant number J2023124. Jing Guo received this grant, the URLs of sponsors' website is https://kxjst.jiangsu.gov.cn/ (accessed on 06 June 2024).

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Jing Guo, Ziying Wang; data collection: Jing Guo, Yajuan Guo; analysis and interpretation of results: Jing Guo, Ziying Wang, Yajuan Guo; draft manuscript preparation: Jing Guo, Haitao Jiang. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data that support the findings of this study are available from the corresponding author Jing Guo upon reasonable request.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

[1] L. Zhang and T. Ponomarenko, "Directions for sustainable development of china's coal industry in the post-epidemic era," *Sustainability*, vol. 15, no. 8, 2023, Art. no. 6518. doi: 10.3390/su15086518.

[2] Y. Y. Zhao *et al.*, "A review on battery market trends, second-life reuse, and recycling," *Sustain. Chem.*, vol. 2, no. 1, pp. 167–205, 2021. doi: 10.3390/suschem2010011.

[3] S. M. Parsa *et al.*, "Lithium-ion battery thermal management via advanced cooling parameters: State-of-the-art review on application of machine learning with exergy, economic and environmental analysis," *J. Taiwan Inst. Chem. Eng.*, vol. 148, 2023, Art. no. 104854. doi: 10.1016/j.jtice.2023.104854.

[4] F. T. Hesary, K. Dong, C. Zhao, and H. Phoumin, "Can financial and economic means accelerate renewable energy growth in the climate change era? The case of China," *Econ. Anal. Policy*, vol. 78, no. 10, pp. 730–743, 2023. doi: 10.1016/j.eap.2023.04.013.

[5] C. Zhao, K. Dong, Z. Liu, and X. Ma, "Is digital economy an answer to energy trilemma eradication? The case of China," *J. Environ. Manag.*, vol. 349, no. 2, 2024, Art. no. 119369. doi: 10.1016/j.jenvman.2023.119369.

[6] I. Mahmud, M. B. Medha, and M. Hasanuzzaman, "Global challenges of electric vehicle charging systems and its future prospects: A review," *Res. Transport. Business Manag.*, vol. 49, no. 1, 2023, Art. no. 101011. doi: 10.1016/j.rtbm.2023.101011.

[7] P. Alaee, J. Bems, and A. Anvari-Moghaddam, "A review of the latest trends in technical and economic aspects of EV charging management," *Energies*, vol. 16, no. 9, 2023, Art. no. 3669. doi: 10.3390/en16093669.

[8] A. Unterweger, F. Knirsch, D. Engel, D. Musikhina, A. Alyousef and H. de Meer, "An analysis of privacy preservation in electric vehicle charging," *Energy Inform.*, vol. 5, no. 3, 2022, Art. no. 2615. doi: 10.1186/s42162-022-00190-y.

[9] J. M. Clairand, J. R. García, and C. Alvarez-Bel, "Smart charging for electric vehicle aggregators considering users' preferences," *IEEE Access*, vol. 6, pp. 54624–54635, 2018. doi: 10.1109/ACCESS.2018.2872725.

[10] Y. He, C. Zhang, B. Wu, Z. Geng, K. Xiao and H. Li, "A trusted architecture for EV shared charging based on blockchain technology," *High-Confid. Comput.*, vol. 1, no. 2, 2021, Art. no. 100001. doi: 10.1016/j.hcc.2021.100001.

[11] D. Kern and C. Krauß, "Detection of e-mobility-based attacks on the power grid," presented at the 2023 53rd Annual IEEE/IFIP Int. Conf. Depend. Syst. Netw., Porto, Portugal, Jun. 27–30. doi: 10.1109/DSN58367.2023.00042.

[12] A. P. Diaz, E. H. Gerding, and F. McGroarty, "Catching cheats: Detecting strategic manipulation in distributed optimisation of electric vehicle aggregators," *J. Artif. Intell. Res.*, vol. 67, pp. 437–470, 2020. doi: 10.1613/jair.1.11573.

[13] M. Ghafouri *et al.*, "Detection and mitigation of cyber attacks on voltage stability monitoring of smart grids," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5227–5238, 2020. doi: 10.1109/TSG.2020.3004303.

[14] M. Keshk, E. Sitnikova, N. Moustafa, J. Hu, and I. Khalil, "An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems," *IEEE Trans. Sustain. Comput.*, vol. 6, no. 1, pp. 66–79, 2021. doi: 10.1109/TSUSC.2019.2906657.

[15] P. R. Badu, B. Palaniswamy, A. G. Reddy, V. Odelu, and H. S. Kim, "A survey on security challenges and protocols of electric vehicle dynamic charging system," *Secur. Privacy*, vol. 5, no. 3, 2022, Art. no. e210. doi: 10.1002/spy2.21.

[16] Y. Chen, Y. Zhang, S. Maharjan, M. Alam, and T. Wu, "Deep learning for secure mobile edge computing in cyber-physical transportation systems," *IEEE Network*, vol. 33, no. 4, pp. 36–41, 2019. doi: 10.1109/MNET.2019.1800458.

[17] A. R. Kizhakkan, A. K. Rathore, and A. Awasthi, "Review of electric vehicle charging station location planning," in *2019 IEEE Transport. Electrif. Conf.*, Bengaluru, India, Dec. 17–19, 2019, pp. 1–5. doi: 10.1109/ITEC-India48457.2019.ITECINDIA2019-226.

[18] K. R. Mestav, X. Wang, and L. Tong, "A deep learning approach to anomaly sequence detection for high-resolution monitoring of power systems," *IEEE Trans. Power Syst.*, vol. 38, no. 1, pp. 4–13, 2022. doi: 10.1109/TPWRS.2022.3168529.

[19] S. M. Miraftabzadeh, C. G. Colombo, M. Longo, and F. Foiadelli, "K-means and alternative clustering methods in modern power systems," *IEEE Access*, vol. 11, pp. 119596–119633, 2023. doi: 10.1109/ACCESS.2023.3327640.

[20] Q. Feng, H. Li, Y. Zhou, D. Feng, Y. Wang and Y. Su, "Review of electric vehicles' charging data anomaly detection based on deep learning," in *2022 Power System and Green Energy Conf.*, Shanghai, China, Aug. 25–27, 2022, pp. 337–341. doi: 10.1109/PSGEC54663.2022.9881073.

[21] A. Haldorai, R. B.Lincy, S. Murugan, and M. Balakrishnan, "A review on smart charging approaches for electric vehicle," *Artif. Intell. Sustain. Develop.*, vol. 9, pp. 177–196, 2024. doi: 10.1007/978-3-031-53972-5_9.

[22] A. Tang, Y. Jiang, Q. Yu, and Z. Zhang, "A hybrid neural network model with attention mechanism for state of health estimation of lithium-ion batteries," *J. Energ. Storage*, vol. 68, no. 4, 2023, Art. no. 107734. doi: 10.1016/j.est.2023.107734.

[23] M. M. Badr, M. I. Ibrahem, H. A. Kholidy, M. M. Fouda, and M. Ismail, "Review of the data-driven methods for electricity fraud detection in smart metering systems," *Energies*, vol. 16, no. 6, 2023, Art. no. 2852. doi: 10.1016/j.est.2023.107734.

[24] A. Bott, T. Janke, and F. Steinke, "Deep learning-enabled MCMC for probabilistic state estimation in district heating grids," *Appl. Energy*, vol. 336, no. 9, 2023, Art. no. 120837. doi: 10.1016/j.apenergy.2023.120837.

[25] B. Li *et al.*, "A method for parameter identification of distribution network equipment based on sequential model-based optimization," *Int. Trans. Electr. Energy Syst.*, vol. 2022, no. 1, 2022, Art. no. 9880284. doi: 10.1155/2022/5358965.

[26] Z. He *et al.*, "A spatiotemporal deep learning approach for unsupervised anomaly detection in cloud systems," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 34, no. 4, pp. 1705–1719, 2020. doi: 10.1109/TNNLS.2020.3027736.

[27] Y. Ji and X. Li, "An efficient intrusion detection model based on deepFM," in *2020 IEEE 4th Inform. Technol. Netw. Electron. Autom. Control Conf. (ITNEC)*, Chongqing, China, Jun. 12–14, 2020, pp. 778–783. doi: 10.1109/ITNEC48623.2020.9084722.

[28] K. Hu, D. Sun, and Y. Zhao, "Enhanced single-frame interferometry via hybrid conv-transformer architecture for ultra-precise phase retrieval," *Opt. Express.*, vol. 32, no. 17, pp. 30226–30241, 2024. doi: 10.1364/OE.530142.