Physics-Informed Learning-based Attack Analytics for Electric Vehicle Charging Management Systems

David Perry*, Mohammad Zakaria Haider*, Kumail Kazmi*,
Mohammad Ashiqur Rahman* and, Hossain Shahriar †
*Analytics for Cyber Defense (ACyD) Lab, Florida International University, USA
†Center for Cybersecurity, University of West Florida, USA
{dperr040, mhaid010, mkazm004, marahman}@fiu.edu, hshahriar@uwf.edu

Abstract—**This work introduces a novel physics-informed neural network (PINN)-based framework for modeling and optimizing false data injection (FDI) attacks on electric vehicle charging station (EVCS) networks, with a focus on centralized charging management system (CMS). By embedding the governing physical laws as constraints within the neural network's loss function, the proposed framework enables scalable, real-time analysis of cyber-physical vulnerabilities. The PINN models EVCS dynamics under both normal and adversarial conditions while optimizing stealthy attack vectors that exploit voltage and current regulation. Evaluations on the IEEE 33-bus system demonstrate the framework's capability to uncover critical vulnerabilities. These findings underscore the urgent need for enhanced resilience strategies in EVCS networks to mitigate emerging cyber threats targeting the power grid. Furthermore, the framework lays the groundwork for exploring a broader range of cyber-physical attack scenarios on EVCS networks, offering potential insights into their impact on power grid operations. It provides a flexible platform for studying the interplay between physical constraints and adversarial manipulations, enhancing our understanding of EVCS vulnerabilities. This approach opens avenues for future research into robust mitigation strategies and resilient design principles tailored to the evolving cybersecurity challenges in smart grid systems.**

Index Terms—**Cybersecurity, False Data Injection, Electric Vehicle Charging Station, Charging Management Systems, Open Charge Point Protocol, Physics-Informed Neural Network**

I. Introduction

A. Motivation

The electrification of transportation has witnessed unprecedented growth in recent years, with electric vehicle charging stations (EVCSs) emerging as a critical component of the electric vehicle (EV) ecosystem. Integrating these charging stations into the power grid introduces a new dimension of cyber-physical interdependence, underscoring the necessity for robust cybersecurity measures. Among the myriad threats facing EVCS, false data injection (FDI) attacks pose a particularly insidious risk, potentially compromising the integrity and functionality of these critical systems. Recently, power grids have become smarter and more efficient by incorporating the internet of things (IoT), making them vulnerable to cyberattacks. A recent report found that the California power grid has defended over a million cyberattacks each month [1]. FDI attacks represent a sophisticated cyber threat in which adversaries manipulate data within a system to deceive its decision-making processes. In the context of EVCS, these attacks can lead to incorrect charging parameters, affecting the state of charge (SoC) and current reference values, compromising the efficiency of the charging process and potentially causing damage to the battery of the electric vehicle [2].

Trends in electrification suggest that one in three cars are expected to be electrified by 2040 [3]. The current EV charging infrastructure has to be improved and expanded in accordance with the global auto fleet's shift toward EVs. The motivations behind cyberattacks on an EVCS range from identity theft and electricity theft to ransomware and virus assaults that potentially compromise the entire EVCS network [4]. The transition of the attack vector from the cyber layer to the physical infrastructure layer involves intricate metrics that should be analyzed with respect to the aftermath in real physical entities such as power, current, voltage, and SoC. The work in [5] includes the vulnerability analysis and risk assessment of an EVCS with details of potential attack scenarios, such as denial of service (DoS), man-in-the-middle (MiTM), and FDI. Ting at el. [6] showed that the abundance of EVs can be exploited to target the stability of the power grid. The adverse interaction between EVCSs and power grids has been presented in [7]–[9]. The scope of this paper will primarily focus on FDI attacks.

Cyber-physical system (CPS) security research in EVCS faces significant challenges due to limited access to the operational model and ethical constraints against real-world testing. The interconnected nature of modern power grids complicates attack vector identification, as disruptions can cascade through systems. While traditional attack analytics models often fail to capture real-world dynamics due to data quality limitations, physics-informed neural networks (PINNs) offer a superior alternative by embedding governing equations directly into their architecture. PINNs enforce conservation laws and system constraints through physics-informed loss functions, eliminating reliance on historical data. Our methodology leverages PINNs as surrogate models to identify adaptive FDI attack vectors in EVCSs, a critical component of the smart grid, with impacts verified by real hardware prototyping.

B. Related Works

Intelligent and adaptive FDI attacks on EVCSs pose significant analytical challenges. Traditional mixed-integer linear programming (MILP) approaches fail to capture non-linear relationships between EVCS networks and power grids, proving computationally prohibitive for systems governed by complex ODEs and PDEs. While conventional machine learning offers robust analytical tools, deep learning provides superior capabilities for complex pattern recognition in grid dynamics, as demonstrated in recent EV charging schemes incorporating renewable energy and dynamic pricing. Physics-informed machine learning further enhances these capabilities by embedding system constraints directly into the learning process, enabling data-efficient representations of system behavior. Recent studies in [10]–[12] have demonstrated the utility of PINNs in modeling non-linear dynamic equations across various domains. The study in [13] presents a novel method for solving the optimal power flow (OPF) problem using physics-informed typed graph neural networks (PI-TGNs). Leveraging PINNs could lead to accurate impact assessments and robust defenses against FDI attacks in modern energy systems. The authors in [14]–[17] discussed challenges PINNs address, including data scarcity, interpretability, and physical consistency, providing a roadmap for future research that leverages PINNs to improve power grid performance and resilience. Researchers in [18] introduced a robust voltage control method for distribution systems using physics-informed graphical representation. The study in [19] presents a hybrid control architecture combining PINNs with model predictive control (MPC) for DC-DC buck converters.

The ever-expanding EV infrastructure has prompted various approaches to managing the penetration of EVs on the power grid. CMS allows monitoring of charging station activity – charging, discharging, scheduling, and load balancing. Cyber-physical security challenges in extreme fast charging (XFC) stations for EVs, focusing on potential cyber threats that could destabilize charging networks and impact grid stability, have been demonstrated in [20]–[23]. Acharya et al. in [24] examined the cybersecurity vulnerabilities arising from integrating EV, EVCS, and the power grid. It highlights risks at the intersection of these systems, including data manipulation, unauthorized access, and potential large-scale demand-side attacks. The study in [25] investigated how botnets composed of compromised EVs and fast-charging stations could impact power grid stability. By analyzing the IEEE 33-bus, the work demonstrated that simultaneous charging via a botnet attack could lead to various harms, including line congestion and voltage drops.

C. *Contributions*

Literature reveals significant gaps in EVCS security, particularly in real-time attack detection and mitigation. Traditional solvers like Gurobi and CPLEX struggle with highly nonlinear systems due to convergence issues, computational demands, and discretization-related errors. In contrast, our proposed model incorporates governing equations directly into neural network architecture, enabling continuous solution approximation without discretization constraints. This approach allows comprehensive exploration of potential attack vectors while ensuring physical plausibility, thereby enhancing detection accuracy and reducing false positives in EVCS networks. Our key contributions in this research can be presented as follows:

- We propose the attack analytics model leveraging PINNs to overcome the limitations of discretization. PINNs explore the continuous attack space without requiring predefined assumptions or resolution, offering a scalable and efficient alternative. By embedding physical laws into the optimization process, PINNs ensure the identified attack vectors remain realistic and actionable, reducing false positives and enhancing the reliability of the analysis.
- Integrating gradient-based optimization to identify attack vectors that maximize performance deviations, such as voltage regulation errors or current disruptions. This approach avoids the computational overhead of discretization and provides a direct solution to ordinary differential equations (ODEs), enabling more efficient and accurate attack modeling.
- Traditional discretization methods, which predefine a limited set of attack scenarios or states, face significant challenges in simulating and analyzing the high-dimensional and continuous nature of attack impacts on EVCS networks. These methods are computationally expensive, scale poorly with system complexity, and struggle to capture subtle but impactful attack vectors. This approach enables accurate modeling of EVCS networks without pre-collected training data, resulting in faster training and improved generalization.

The rest of the paper is organized as follows: we have discussed the technical overview of the system in Section II. Section III discusses the modeling of the optimal attack analytics model. Section IV explains testbed implementation that validates the PINN framework against real EVCS controllers under various scenarios. Section V discusses performance evaluation and the impact of FDI attacks on the EVCS network. Finally, we conclude the paper in Section VI.

II. Technical Overview

A. *EVCS Dynamics*

AC-to-DC power conversion for EV charging involves multiple stages to ensure safe and efficient operation. Grid synchronization, managed by a phase-locked loop (PLL), aligns the control system with grid voltage by continuously adjusting for grid angle and frequency discrepancies. The rectified AC power is stored in a DC link, where a control loop stabilizes voltage by minimizing fluctuations from grid disturbances or load variations. Reference currents for direct and quadrature AC components are computed for current regulation managed by an inner loop compensating for component resistance and inductance. An LCL filter smooths AC currents and removes harmonics before rectification. The DC-link balances power input from the grid with EV consumption, while a DC-DC converter modulates the stabilized voltage to match the EV battery's requirements. This ensures precise, reliable, and

TABLE I
MODELING NOTATIONS

Type of Notation	Notation	Description
General	$\mathcal{B}$	Set of all buses in the system
	$\mathcal{B}^{EV}$	Set of EVCS buses
	$\mathcal{T}$	Set of all timeslots for controller's response
	b, i	indices for buses
Bus Measurements	δ	Phase angle of bus
	$\mathcal{V}_t$	Bus voltage
	$\mathcal{F}_t$	Bus Frequency
EVCS Measurements	P	Active power
	$\mathbf{Q}$	Reactive power
	δ	Phase angle
	ω	Angular frequency
	$\mathbf{v}_{dc}$	DC link voltage of converter
	$\mathbf{v}_{out}$	Output/terminal voltage of EVCS
	$\mathbf{v}_{ref}$	Reference setpoints of AC/DC converter voltage
	$\mathbf{i}_{dc}$	DC link current of converter
	$\mathbf{i}_{out}$	Output/terminal current of EVCS
	$\mathbf{i}_{ref}$	Reference setpoints of AC/DC converter current
	$\mathbf{m}_{vdc}$	Modulation index of AC/DC converter
	ϕ_d	d-axis flux linkage
	ϕ_q	q-axis flux linkage
Fixed Parameters	$\mathbf{R}$	Line resistance
	$\mathbf{L}$	Inductance of LCL filter
	$\mathbf{C}$	Capacitance of LCL filter
ADM Parameter	$\tau_{V_{\text{out}}}$	ADM threshold for voltage
	$\tau_{I_{\text{out}}}$	ADM threshold for current
	$\mathbf{P}^{min,max}$	ADM threshold for active power
	$\mathbf{Q}^{min,max}$	ADM threshold for reactive power

efficient charging, safeguarding battery health and maintaining overall system stability. The EVCS dynamics used for this attack analytics model are discussed in [26]. The modeling notations for power system components, dynamics, and FDI attacks are mentioned in Table I.

B. Charging Management System

CMS ensures the stability of the EVCS network by continuously monitoring voltages and currents, comparing them with setpoints, and issuing corrective signals to local controllers. By coordinating multiple EVCS units, the CMS prevents localized disturbances from affecting the wider network. The PINNs model optimizes controller gains to counter cyber-physical threats, enhancing system stability and security as EV adoption grows. CMS uses proportional integral (PI) controllers to regulate voltage and current within limits. However, if attackers inject false data by bypassing anomaly detection, the CMS can be misled to issue incorrect setpoints, destabilizing the voltage.

C. Loss Functions for PINN Model

The loss function is crucial in training PINNs, integrating physical laws, and data-driven objectives to model complex systems accurately. It enforces governing equations as penalty terms, ensuring that predictions align with system dynamics while reducing dependence on large datasets. Additional terms for boundary, initial conditions, and data consistency refine accuracy. The multi-objective structure enables PINNs to handle high-dimensional, nonlinear systems without traditional discretization, enhancing scalability. Proper weighting of loss terms ensures a balance between physical constraints and empirical data, making PINNs a powerful tool for modern scientific and engineering challenges. One of the major loss functions, PINN needs to minimize is the mismatch of active and reactive power. If $\mathcal{L}_{\text{PF}}$ represents the **power flow loss** the loss function can be written as:

$$\mathcal{L}_{\text{PF}} = \sum_{i=1}^{N} \sum_{j \in \mathcal{N}_i} \left(P_{ij}^{\text{actual}} - P_{ij}^{\text{expected}} \right)^2 \tag{1}$$

Voltage regulation loss ensures the voltage at each bus stays within a specified range (i.e., (V_{lower} - V_{upper}). If $\mathcal{L}_{\text{VR}}$ represents the **voltage regulation loss**, then it can be calculated as:

$$\mathcal{L}_{\text{VR}} = \sum_{i=1}^{N} \left(\max(0, V_i - V_{\max}) + \max(0, V_{\min} - V_i) \right)^2 \tag{2}$$

The loss terms related to EVCS capture the dynamics of the EVCS system. Each time derivative is associated with a loss term that penalizes deviations from its expected value. Each loss function targets a specific parameter to ensure it aligns closely with its desired trajectory or calculated value based on system equations. The loss function for the phase angle ensures that the rate of change of the phase angle matches the system's angular frequency and can be written as:

$$\frac{d\delta}{dt}_{loss} = \left(\frac{d\delta}{dt} - \omega \right)^2 \tag{3}$$

The loss function of the phase-locked loop (PLL) error minimizes the discrepancies of the AC-DC converter. The equation can be written as:

$$\frac{d\omega}{dt}_{loss} = \left(\frac{d\omega}{dt} - PLL_{error} \right)^2 \tag{4}$$

The flux linkage components are governed by the following loss functions:

$$\frac{d\phi}{dt} loss = \left(\frac{d\phi_j}{dt} - v_j \right)^2 ; i = q, d \tag{5}$$

These ensure alignment between the rate of change of flux linkages and the respective voltage components. d-axis and q-axis current dynamics are managed by:

$$\frac{di_j}{dt}_{loss} = \left(\frac{di_j}{dt} - \frac{1}{L_{L1}} \left(v_j^{conv} - R \cdot i_j - v_j + \omega L_{L1} \cdot i_k \right) \right)^2 \tag{6}$$

where j, k q-axis, and d-axis are components of converter current. These ensure that the currents in the d- and q-axes align with their expected dynamic behavior. The inductor current and capacitor voltage dynamics of the LCL filter used in the system are described as follows:

$$\frac{di_{L_1}}{dt}_{loss} = \left(\frac{di_{L_1}}{dt} - \frac{1}{L_{L_1}}\left(v_d^{conv} - v_c - R \cdot i_{L_1}\right)\right)^2 \tag{7}$$

$$\frac{di_{L_2}}{dt}_{loss} = \left(\frac{di_{L_2}}{dt} - \frac{1}{L_{L_2}}\left(v_c - v_{ac} - R \cdot i_{L_2}\right)\right)^2 \tag{8}$$

$$\frac{dv_c}{dt}_{loss} = \left(\frac{dv_c}{dt} - \frac{1}{C_{L1}}\left(i_{L_1} - i_{L_2}\right)\right)^2 \tag{9}$$

$$\frac{dv_{dc}}{dt}_{loss} = \left(\frac{dv_{dc}}{dt} - \frac{1}{v_{dc} \cdot C_{dc}}\left(P_{\text{ac}} - v_{dc} \cdot i_{dc}\right)\right)^2 \tag{10}$$

The overall loss of an EVCS is the summation of the individual loss of each EVCS, and if $\mathcal{L}_{\text{EVCS}}$ represents the **total EVCS dynamics loss**, then it can be represented as:

$$\mathcal{L}_{\text{EVCS}} = \sum_{i=1}^{N} \left\{ \frac{d\delta}{dt}_{loss} + \frac{d\omega}{dt}_{loss} + \frac{d\phi}{dt}_{loss} + \frac{di_{L_1}}{dt}_{loss} + \frac{di_{L_2}}{dt}_{loss} + \frac{di_{v_c}}{dt}_{loss} + \frac{dv_{dc}}{dt}_{loss} \right. \tag{11}$$

These losses align the inductor current and capacitor voltage with their expected behavior in response to system inputs. The loss functions outlined provide a robust framework for system control, ensuring critical parameters like voltage, current, frequency, and phase angle behave as intended. This mathematical structure is fundamental in implementing control systems for energy networks, particularly in advanced grid operations involving EVCS.

$$\mathcal{L}_{\text{total}} = \lambda_1 \mathcal{L}_{\text{PF}} + \lambda_2 \mathcal{L}_{\text{VR}} + \lambda_3 \mathcal{L}_{\text{EVCS}} \tag{12}$$

Where, $\lambda_1, \lambda_2, \lambda_3$ are weighting factors.

D. PINN Model Structure

We developed an LSTM-based PINNs with four hidden layers of 512 LSTM units each to model the EVCS network dynamics. Leveraging PyTorch's *torch.autograd* for automatic differentiation, the model enforces system equations while capturing non-linear and time-dependent behaviors. Validation under varying load conditions, discussed in Section IV, shows the LSTM-PINN accurately learns temporal dependencies and matches real-world EVCS behavior. Fig. 1 illustrates the architecture of the proposed attack analytics model.

III. Attack Analytics Model

We use PINNs to model the non-linear dynamics of EVCS networks and evaluate the impact of stealthy FDI attacks. The attack model targets OCPP-based CMS interfaces, enabling manipulation of charging parameters (e.g., power flow, current, SoC) while evading detection. Assuming attacker knowledge of EVCS operations, the attack is formulated as a constrained optimization problem to maximize disruption without triggering alarms. PINNs provide a scalable framework to learn system dynamics and identify vulnerabilities in EVCS-enabled distribution grids.

A. Attack Technique

Assume that $\tilde{V}^t_{\text{out},b}$ and $\tilde{I}^t_{\text{out},b}$ are the false data injected into the output voltage and output current measurements of the EVCS converter at node b and time t. The resulting attacked measurements $\bar{V}^t_{\text{out},b}$ and $\bar{I}^t_{\text{out},b}$ can be expressed as:

$$\forall b \in \mathcal{B}, t \in \mathcal{T}, \quad \bar{V}^t_{\text{out},b} = V^t_{\text{out},b} + \tilde{V}^t_{\text{out},b} \tag{13}$$

$$\forall b \in \mathcal{B}, t \in \mathcal{T}, \quad \bar{I}^t_{\text{out},b} = I^t_{\text{out},b} + \tilde{I}^t_{\text{out},b} \tag{14}$$

where $\mathcal{B}$ represents the EVCS nodes and $\mathcal{T}$ denotes the duration of the attack.

B. Attack Optimization

The attacker's goal is to deploy optimized FDI attacks that maximize voltage and current deviations across the EVCS network, degrading control system effectiveness. By incorporating system dynamics into a PINN's loss function, attackers can identify subtle perturbations that exploit physical constraints while evading detection systems. The objective can be formulated as:

$$\max_{\delta V, \delta I} \quad \mathbb{E}\left[\sum_{t=0}^{T} \left(\|V_{\text{out}}(t) - V_{\text{nominal}}(t)\| + \|I_{\text{out}}(t) - I_{\text{nominal}}(t)\|\right)\right] \tag{15}$$

subject to the physical constraints of the EVCS network:

$$\mathcal{F}(V_{\text{out}}, I_{\text{out}}, \delta V, \delta I) = 0 \tag{16}$$

where δV and δI represent the adversarial perturbations introduced to voltage and current measurements, and $\mathcal{F}(\cdot)$ denotes the dynamics of the underlying physics-based system modeled within the PINN framework.

C. Attack Constraints

The attacker's ability to manipulate the EVCS network is constrained by two primary factors: accessibility and stealth requirements under the anomaly detection mechanism.

Accessibility: Accessibility defines the EVCS nodes and measurements that the attacker can target, influenced by network topology, open services, and existing security controls. This is represented by a binary vector $\mathbb{A} \in \mathbb{R}^{|\mathcal{B}|}$, where $\mathbb{A}_b = 0$ indicates that the EVCS node b is inaccessible to the attacker.

$$\forall b \in \mathcal{B}, t \in \mathcal{T}^S, \quad \mathbb{A}_b = 0 \rightarrow \Delta V^b_{\text{out},t} = 0,\, \Delta I^b_{\text{out},t} = 0 \tag{17}$$

This constraint ensures that the attacker can only introduce perturbations $\Delta V^b_{\text{out},t}$ and $\Delta I^b_{\text{out},t}$ at nodes where accessibility is granted, preventing modifications to inaccessible EVCS.

Stealth Constraints: To avoid detection by the anomaly detection model (ADM), the attacker keeps the injected deviations $\tilde{V}^b_{\text{out},t}$ and $\tilde{I}^b_{\text{out},t}$ within the tolerable limits of the CMS (i.e. $\tau_{v_{\text{out}}}$, $\tau_{i_{\text{out}}}$). These limits ensure that any sudden change is not possible for the attacker to inject because the CMS checks the variations in consecutive time-steps and discards the values that are out of the threshold values. The constraints on the permissible rate of change between consecutive measurements are mentioned in (18)-(22):

$$-\tau_{V_{\text{out}}} \leq (V^b_{\text{out},t+1} + \tilde{V}^b_{\text{out},t+1}) - (V^b_{\text{out},t} + \tilde{V}^b_{\text{out},t}) \leq \tau_{V_{\text{out}}} \tag{18}$$

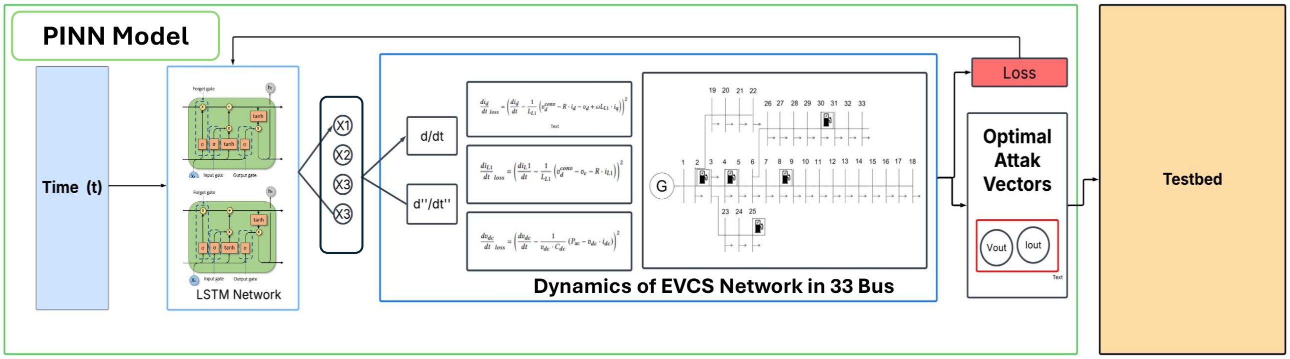


Fig. 1. Deep LSTM-based PINN attack analytics model.

$$-\tau_{I_{\text{out}}} \leq (I^b_{\text{out},t+1} + \tilde{I}^b_{\text{out},t+1}) - (I^b_{\text{out},t} + \tilde{I}^b_{\text{out},t}) \leq \tau_{I_{\text{out}}} \quad (19)$$

$$P_b^{min} \leq P_b[t] \leq \bar{P}_b^{max}, \quad \forall b \in \mathbf{B}^{EV}, \forall t \in \mathbf{T} \quad (20)$$

$$Q_b^{min} \leq Q_b[t] \leq \bar{Q}_b^{max}, \quad \forall b \in \mathcal{B}^{EV}, \forall t \in \mathcal{T} \quad (21)$$

$$V_b^{out,min} \leq V_b^{out}[t] \leq \bar{V}_b^{out,max}, \quad \forall b \in \mathbf{B}^{EV}, \forall t \in \mathbf{T} \quad (22)$$

D. Attack Assumptions

This attack model considers the following assumptions to simulate a worst-case scenario for the EVCS network:

- ***Assumption I:*** The Attacker agents have extensive knowledge of the CMS's control algorithms, EVCS network parameters, and ADM thresholds.
- ***Assumption II:*** Attackers can access voltage V_{out} and current I_{out} measurements from RTUs at selected EVCS buses, but control signals from the charging management system to EVCS converters remain secure.
- ***Assumption III:*** Load conditions across the EVCS network may vary during the attack.
- ***Assumption IV:*** The attacker has sustained access to compromised sensors, enabling continuous monitoring and manipulation of V_{out} and I_{out} across targeted EVCS.

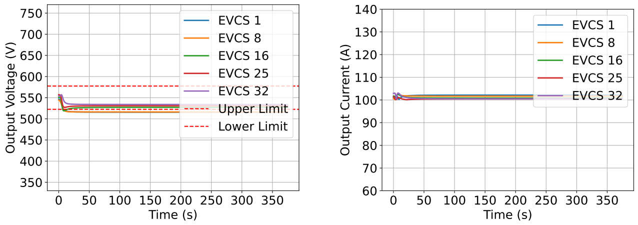
These assumptions provide a detailed foundation for analyzing potential vulnerabilities within the CMS-managed EVCS network under coordinated FDI attacks, specifically on the voltage and current control elements. This analysis highlights the EVCS network's resilience against sophisticated cyber threats and informs strategies to enhance CMS security.

IV. Testbed Design and Experimentation

We first describe the experimental setup which incorporates industry-standard IEEE bus configurations and realistic power electronics modeling. We further demonstrate the behavior of the system in steady-state and dynamic conditions, providing insight into the characteristics of the charging infrastructure.

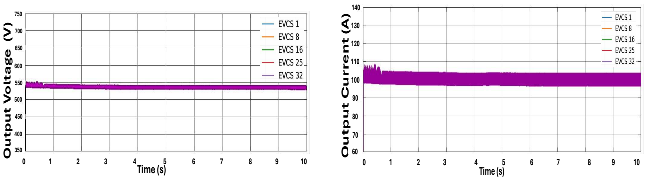
A. Simulation-based Experimentation

Simulation Design: The PINN-based attack analytics model was implemented in Python and executed on an Intel Xeon E5-240 system with dual RTX 4090 GPUs and 248GB RAM. It models the IEEE 33-bus grid with five 55kW EVCS operating at 98% efficiency using per-unit (p.u.) scaling. The environment includes LCL filters, DC-DC converters, and power electronics for accurate power flow simulation. For validation, a Simulink-based EVCS model from [27] was integrated with the IEEE 33-bus system. A PI-based CMS manages the optimal charging of the EVCS across the network.



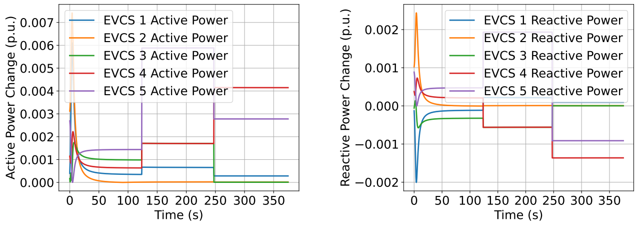
(a) (b)

Fig. 2. PINN outputs of EVCS (a) voltage, (b) current in steady state condition.



(a) (b)

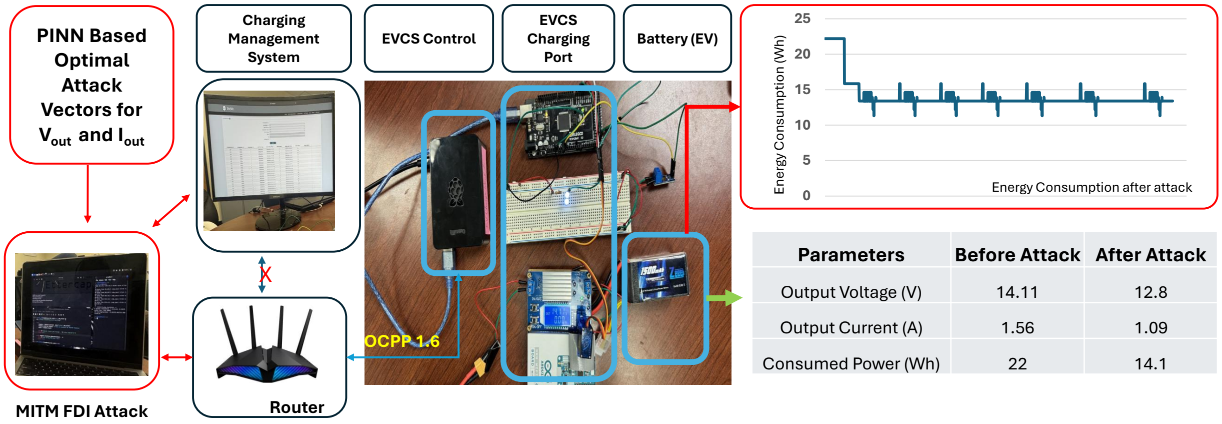
Fig. 3. Simulink outputs of EVCS (a) voltage and (b) current on steady state condition.



(a) (b)

Fig. 4. Demonstrating outputs of EVCS (a) active power and (b) reactive power in EVCS Bus due to change of load.

Steady-State Response: During normal operation, the EVCS voltages demonstrate ideal convergence characteristics, settling


PINN Based Optimal Attack Vectors for V_{out} and I_{out}
Charging Management System
EVCS Control
EVCS Charging Port
Battery (EV)
OCPP 1.6
MITM FDI Attack
Router
Energy Consumption (Wh)
25
20
15
10
5
0
Energy Consumption after attack

Parameters	Before Attack	After Attack
Output Voltage (V)	14.11	12.8
Output Current (A)	1.56	1.09
Consumed Power (Wh)	22	14.1

Fig. 5. Hardware testbed for PINN attack analytics.

precisely at the specified set point. The system response in a steady-state EVCS network is shown in Fig. 2. The figure shows that the system comes to a steady-state position after initial oscillation. The actual values of output voltage, output current, and active power are 550V, 100A, and 55kW, respectively. The steady-state response of EVCS's terminal voltage and current simulated in Simulink are shown in Fig. 3.

Dynamic Response: We introduced up to 20% load variations at EVCS-connected buses in the IEEE 33-bus system to assess power balance and load dynamics. Fig. 4 shows the grid maintains stability by adjusting setpoints and redistributing power, keeping voltage and power flows within limits. These results validate the model's ability to capture realistic EVCS demand and grid interactions.

B. Testbed Validation

The vulnerability of the OCPP module to FDI attacks was assessed using a prototype EVCS connected to a CMS. The hardware setup used for this experiment is illustrated in Fig. 5. The prototype consists of a combination of an Arduino, a DC-DC voltage regulator, voltage and current sensors, and an analog-to-digital converter representing the physical EVCS charging system. In addition to this, a Raspberry Pi was used to represent the EVCS server that communicates with an open-source CMS (SteVe) [28]. The system follows OCPP 1.6J, the industry-standard protocol for bidirectional EVCS-CMS communication, enabling real-time data exchange through WebSocket connections. This facilitates efficient monitoring of charging sessions, including station availability, transactions, power consumption, and SoC updates. The network architecture integrates a SteVe-based CMS running in a modified Docker setup that communicates with the EVCS's components via serial communication. The Raspberry Pi initiates an OCPP transaction, prompting the Arduino to generate a PWM signal for the load (a battery and LED) while the CMS records the total power supplied. For cybersecurity analysis, a Kali Linux virtual machine with Wireshark, Scapy, and Ettercap installed is used for network sniffing, packet analysis, and injection, allowing message monitoring and manipulation within the network. The prototype operates at a voltage of 14.11V and a current of 1.56A. The attack vectors we have derived from our attack analytics model are scaled to this level and injected through the MiTM attack between the EVCS module and CMS. From Fig. 5, we have found that, when the attack values are injected, the voltage drops to 12.8V from 14.11V and the current drops to 1.09A from 1.56A, which in turn drops the power consumed by the battery from 22Wh to 14.1Wh. This validation supports the effectiveness of our attack module.

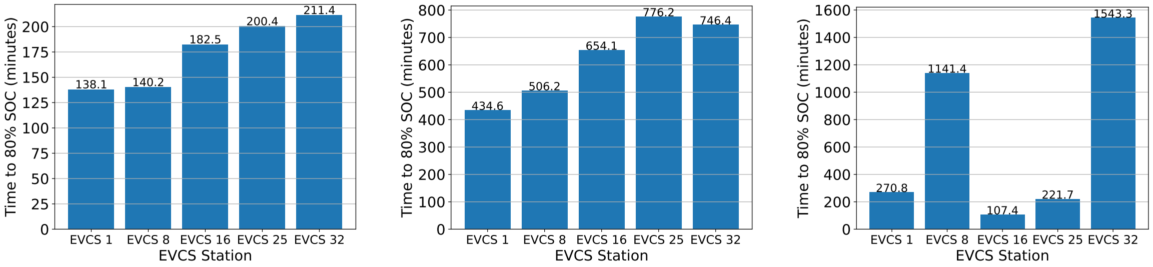
V. Evaluation

This research explores the security of EVCS networks using a PINN-based attack analytics model. To guide our investigation and provide a structured framework for evaluating our proposed methodology, we formulate the following research questions (RQ):

- **RQ1**. *What is the impact of the attack vectors on the charging schedule?*
- **RQ2**. *How scalable are the attack vectors to create disturbances in the EVCS Network?*
- **RQ3**. *How computationally efficient is the PINN-based model in analyzing attack vectors compared to traditional methods?*

A. Impact of Attack on Charging Schedule

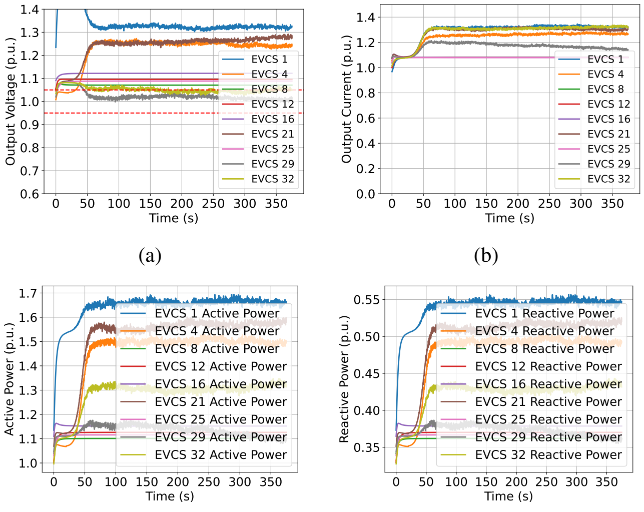
In the steady-state operational regime of an EVCS network, the power distribution remains relatively uniform across all charging nodes, with consistent charging times as illustrated in Fig. 6(a). Under normal conditions, charging times range from approximately 138.3 to 211.5 minutes between stations. However, during peak hours with high load demand (Fig. 6(b)), the CMS dynamically adjusts reference setpoints through closed-loop control mechanisms to optimize power distribution. This results in extended charging durations at individual EVCS locations, with times ranging between 414.6 and 746.4 minutes, nearly twice the normal charging time. Most critically, as demonstrated in Fig. 6(c), sophisticated cyberphysical attacks that stealthily manipulate CMS setpoints can induce severe charging disruptions without actual load



(a) (b) (c)

Fig. 6. Required charging time for 5 EVCS in (a) normal operating conditions, (b) peak hour with high load demand, and (c) under cyber attack.

changes. These attacks extend charging times to over 1500 minutes (7× normal) by forcing false power adjustments. Such manipulation has bidirectional impacts: power reduction leads to grid congestion and service degradation, while overdelivery risks thermal stress, lithium plating, and battery degradation, threatening system safety and reliability.



(a) (b)

(c) (d)

Fig. 7. Results of PINN model for (a) optimal attack value for voltage measurements, (b) EVCS output voltage, (c) EVCS output current, and (d) active power delivered by EVCS while targeting at most 9 EVCS.

B. FDI Attack Impact on CMS

Although the attack analytics model is primarily developed for 5 EVCSs, one of the major advantages is that it can be extended to any number of EVCS. We have simulated the IEEE 33-bus system with up to 15 EVCS to identify optimal attack vectors that could exploit vulnerabilities while remaining undetected. Our approach leveraged the actual dynamics of the system to ensure that the attack vectors maintained both physical plausibility and evasion of the detection mechanisms. The attack vectors were derived through a rigorous process that incorporated the dynamics and constraints of the systems. Our methodology ensured that all vectors adhered to the constraints of the physical system, including power flow equations, voltage, and current limits. Furthermore, vectors operate below established thresholds for anomaly detection systems, making them particularly difficult to identify through conventional monitoring systems. Through systematic analysis of various attack scenarios, we identified optimized stealthy attack vectors that maximize disruption while evading detection. Fig. 7 shows the system's progressive deviation under these attacks, leading to voltage instabilities, power flow shifts, and cascading failures, while keeping individual measurements within normal operational thresholds. Importantly, the PINN framework scales efficiently to larger networks, automatically identifying vulnerable nodes across different EVCS deployment levels, making it a scalable and robust security assessment tool.

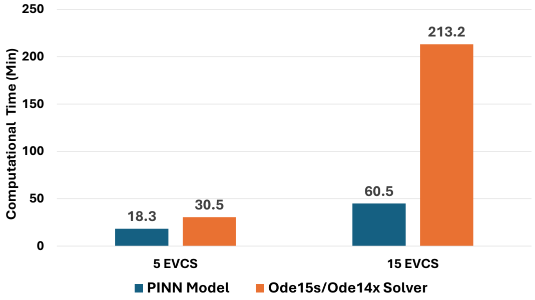


Fig. 8. Comparison of computational time between PINN and Ode14/15 based solver models.

C. Computational Advantage

We performed a computational analysis of the IEEE 33-bus system with EVCS integration, comparing PINNs with traditional solvers (Ode14/Ode15s). The PINN model ran 1.5× faster for 5 EVCSs and 6.5× faster for 15 EVCSs, as shown in Fig. 8. Unlike sequential numerical solvers, PINNs leverage parallelizable neural architectures, reducing bottlenecks when handling stiff system dynamics. Notably, these gains were achieved without GPU acceleration, highlighting the algorithmic efficiency of PINNs over traditional methods. This performance improvement is primarily due to the parallelizable architecture of neural networks, which allows simultaneous evaluation of system dynamics across multiple time steps, bypassing the sequential nature of adaptive step-size solvers like Ode14 and Ode15s. While traditional solvers require iterative error estimation and correction at every step, PINNs approximate the solution across the entire domain in a single forward pass, significantly reducing computation overhead.

VI. Conclusion

Our research introduces a PINNs framework for modeling FDI attacks on EVCS networks. By embedding physical laws directly into neural networks, we overcome limitations of traditional discretization methods, enabling continuous, scalable analysis of cyber-physical vulnerabilities. The framework efficiently identifies attack vectors that maximize voltage regulation errors and current disruptions while maintaining stealth against conventional detection systems. Our gradient-based optimization directly solves governing ODEs without computational overhead, providing superior precision compared to conventional approaches that struggle with scalability in complex systems. These findings highlight the urgent need for enhanced resilience in EVCS infrastructure and position PINNs as a robust foundation for developing physics-aware defense mechanisms to protect increasingly complex power grid systems against sophisticated cyber threats.

Acknowledgment

This research was supported by the award #2433800 and #1946442 from the National Science Foundation (NSF), as well as the award #DE-CR0000024 and #DE-NA0004016 from the Department of Energy (DOE). Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF and DOE.

References

[1] (2019) California operator of electricity grid fends off millions of cyberattacks each month. [online].available: https://www.sandiegouniontribune.com/business/energy-green/story/2019-06-12/california-grid-operator-a-target-for-millions-of. 2019.

[2] Muhammad Shahid Mastoi, Shenxian Zhuang, Hafiz Mudassir Munir, Malik Haris, Mannan Hassan, Muhammad Usman, Syed Sabir Hussain Bukhari, and Jong-Suk Ro. An in-depth analysis of electric vehicle charging station infrastructure, policy implications, and future trends. *Energy Reports*, 8:11504–11529, 2022.

[3] Zacharenia Garofalaki, Dimitrios Kosmanos, Sotiris Moschoyiannis, Dimitrios Kallergis, and Christos Douligeris. Electric vehicle charging: A survey on the security issues and challenges of the open charge point protocol (ocpp). *IEEE Communications Surveys Tutorials*, 24(3):1504–1533, 2022.

[4] Manoj Basnet and Mohd. Hasan Ali. Deep learning-based intrusion detection system for electric vehicle charging station. In *Proc. 2020 2nd International Conference on Smart Power Internet Energy Systems (SPIES)*, pages 408–413, 2020.

[5] Devin Reeh, Francisco Cruz Tapia, Yu-Wei Chung, Behnam Khaki, Chicheng Chu, and Rajit Gadh. Vulnerability analysis and risk assessment of ev charging system under cyber-physical threats. In *2019 IEEE Transportation Electrification Conference and Expo (ITEC)*, pages 1–6, 2019.

[6] Ting Yan, Ziwei He, Nan Zhao, Zhijun Zhang, and Tingjun Zhang. Coordinated charging and discharging of electric vehicles for power imbalance mitigation. In *Proc. 2021 International Conference on Power System Technology (POWERCON)*, pages 778–783, 2021.

[7] Aiguo Cai, Yannan Yu, Liang Xu, Yunbo Niu, and Jichi Yan. Review on reactive power compensation of electric vehicle charging piles. In *Proc. 2019 22nd International Conference on Electrical Machines and Systems (ICEMS)*, pages 1–4, 2019.

[8] Feng Chen, Li Ruijie, and Liu Guanhua. Research on harmonic analysis and harmonic suppression measures of electric vehicle charging station. In *Proc. 2019 IEEE 2nd International Conference on Automation, Electronics and Electrical Engineering (AUTEEE)*, pages 71–75, 2019.

[9] Mithat C. Kisacikoglu, Burak Ozpineci, and Leon M. Tolbert. Reactive power operation analysis of a single-phase ev/phev bidirectional battery charger. In *Proc. 8th International Conference on Power Electronics - ECCE Asia*, pages 585–592, 2011.

[10] Xiaofeng Li. Physics informed neural network based deep adaptive sampling technique for partial differential equations solving. In *Proc. 2024 Third International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, pages 1–4, 2024.

[11] Likun Chen, Xuzhu Dong, Yifan Wang, Wei Sun, Bo Wang, and Gareth Harrison. Physics-informed neural network for microgrid forward/inverse ordinary differential equations. In *Proc. 2024 IEEE Power Energy Society General Meeting (PESGM)*, pages 1–5, 2024.

[12] Junjun Yan, Xinhai Chen, Zhichao Wang, Enqiang Zhoui, and Jie Liu. St-pinn: A self-training physics-informed neural network for partial differential equations. *2023 International Joint Conference on Neural Networks (IJCNN)*, pages 1–8, 2023.

[13] Tania B. Lopez-Garcia and Jose A. Dominguez-Navarro. Optimal power flow with physics-informed typed graph neural networks. *IEEE Transactions on Power Systems*, 2024.

[14] Bin Huang and Jianhui Wang. Applications of physics-informed neural networks in power systems - a review. *IEEE Transactions on Power Systems*, 38(1):572–584, 2023.

[15] Huynh T. T. Tran and Hieu T. Nguyen. Modeling power systems dynamics with symbolic physics-informed neural networks. In *Proc. 2024 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, pages 1–6, 2024.

[16] Raju Gottumukkala, Rizwan Merchant, Adam Tauzin, Kaleb Leon, Andrew Roche, and Paul Darby. Cyber-physical system security of vehicle charging stations. In *Proc. 2019 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 1–6, 2019.

[17] Samrat Acharya, Yury Dvorkin, Hrvoje Pandžić, and Ramesh Karri. Cybersecurity of smart electric vehicle charging: A power grid perspective. *IEEE Access*, 8:214434–214447, 2020.

[18] Di Cao, Junbo Zhao, Jiaxiang Hu, Yansong Pei, Qi Huang, Zhe Chen, and Weihao Hu. Physics-informed graphical representation-enabled deep reinforcement learning for robust distribution system voltage control. *IEEE Transactions on Smart Grid*, 15(1):233–246, 2024.

[19] Peifeng Hui, Chenggang Cui, Pengfeng Lin, Chuanlin Zhang, Kanghua Xu, Amer M. Y. M. Ghias, Hui Chen, and Xitong Niu. Physics-informed neural network model predictive control research on control strategy of dc-dc buck converter. In *Proc. 9th Asia Conference on Power and Electrical Engineering (ACPEE)*. IEEE, 2024.

[20] Mansi Girdhar, Junho Hong, Hyojong Lee, and Tai-Jin Song. Hidden markov models-based anomaly correlations for the cyber-physical security of ev charging stations. *IEEE Transactions on Smart Grid*, 13(5):3903–3915, 2022.

[21] Zoya Pourmirza and Sara Walker. Electric vehicle charging station: Cyber security challenges and perspective. In *Proc. 2021 IEEE 9th International Conference on Smart Energy Grid Engineering (SEGE)*, pages 111–115, 2021.

[22] Aiguo Cai, Yunbo Niu, Yannan Yu, Jichi Yan, and Liang Xu. Review on reactive power compensation of electric vehicle charging piles. In *Proc. 2019 IEEE 22nd International Conference on Electrical Machines and Systems (ICEMS)*, pages 1–7, 2019.

[23] Mohammad Ali Sayed, Mohsen Ghafouri, Mourad Debbabi, and Chadi Assi. Dynamic load-altering ev attacks against power grid frequency control. In *Proc. 2022 IEEE Power Energy Society General Meeting (PESGM)*, pages 1–5, 2022.

[24] Samrat Acharya, Yury Dvorkin, Hrvoje Pandžić, and Ramesh Karri. Cybersecurity of smart electric vehicle charging: A power grid perspective. *IEEE Access*, 8:214434–214449, 2020.

[25] Omniyah Gul M Khan, Ehab El-Saadany, Amr Youssef, and Mostafa Shaaban. Impact of electric vehicles botnets on the power grid. In *Proceedings of the IEEE Conference on Power Systems*. IEEE, 2023.

[26] Amit Kumer Podder, Tomonori Sadamoto, and Aranya Chakrabortty. Optimal charging control and incentivization strategies for electric vehicles considering grid dynamical constraints. In *2024 American Control Conference (ACC)*, pages 3728–3733, 2024.

[27] DC Fast Charger for Electric Vehicle. [online].available: https://www.mathworks.com/help/sps/ug/dc-fast-charger.html. 2023.

[28] RWTH Aachen University. https://github.com/steve-community/steve, 2013.