Design of Joint Cyber-Attacks on Electric Vehicle Charging via Pricing and Traffic Manipulation to Threaten Secure Operation of Power Systems

Runzhuo Ma Siqi Bu, *Senior Member, IEEE*

***Abstract*—The rapid development of electric vehicles (EVs) has strengthened the coupling between transportation and power systems. Meanwhile, the continuous growth in demand for EV charging would significantly impact the secure operation of power systems. Considering the vulnerability of vehicle navigation communication networks, this paper proposes a novel and practical joint cyber-attack scheme to manipulate the charging and route planning results of EV charging navigation. This cyber-attack can minimize both the charging price at the target EV charging station (EVCS) and the driving time required to reach the target EVCS, thus threatening the secure operation of power systems by attracting excessive EVs to charge at the target EVCS. Firstly, a two-level optimization model is proposed to identify the target EVCS based on the partially observable distribution network. This model identifies the EVCS that pose the greatest threat to the secure operation of power systems. Subsequently, a cyber-attack model is developed to manipulate the driving time of EVs to the target EVCS. The attack vector is designed to be stealthy to evade detection and sparse to minimize attack cost. Finally, based on the relationship between charging price and demand, an adaptive cyber-attack model for EV charging price is designed. When the joint cyber-attack is launched, EVs can be reasonably attracted to the target EVCS, regardless of the charging preferences of EV drivers. The coupled test system consisting of an IEEE 33-bus system and a 46-node transportation system verifies the effectiveness of the proposed methodology and model.**

***Index Terms*—Cyber-attacks, electric vehicle (EV), electric vehicle charging navigation system (EVCNS), charging price, route planning**

I. Introduction

To achieve sustainable development goals, countries around the world are vigorously promoting various technologies and policies that reduce energy consumption and carbon emissions [1]. Promoted by market and relevant policies, transportation electrification is developing rapidly as an effective environmental protection method [2]. This will facilitate the coupling of cyber-physical transportation systems (CPTSs) and cyber-physical power systems (CPPSs) to form a complex cyber-physical system [3], [4]. EVs can help CPPSs increase renewable energy utilization and enhance operational efficiency. However, the increase in heavy loads will change the power demand profile of consumers and pose serious challenges to the operation of CPPSs [5], [6]. It is necessary to pay adequate attention to the secure operation of CPPSs [7].

As the coupling points connecting CPTSs with CPPSs, electric vehicle charging stations (EVCSs) provide a new avenue for launching cyber-attacks on CPPSs. Well-designed cyber-attacks can have a serious impact on CPPSs [8], [9]. EV-driven load manipulations have been shown to induce oscillations in the rotor speeds of multiple generators, which could subsequently result in generator tripping and even provoke cascading failures across the power system [10]. It has further been revealed by Abazari *et al.* that strategically designed cyber-attacks can excite sub-synchronous resonance and damage the turbine-generator shafts of synchronous generators [11]. An approach have proposed by Kabir *et al.* to disrupt the angular velocity of the generators by switching the injected and absorbed power of the EVs at the inter-area frequency [12]. Based on [12], the distributed characteristics of the EVCS botnet have been further considered, and a load-altering attack against the EVCSs has been launched to cause generator oscillations [13]. It has also been pointed out by An *et al.* that attacks on the vehicle-to-grid measurement process can lead to controller parameter mismatches and serious voltage problems [14]. Nevertheless, the execution of these attacks typically requires access to detailed power system parameters, which are often difficult for attackers to obtain.

On the other hand, to enhance the feasibility of cyber-attacks, a growing body of research has focused on launching attacks under conditions where power system parameters are either unknown or only partially known. In [15], a load-altering attack leveraging EV control and wind variability to disrupt grid frequency has been proposed under partial system knowledge. Under the condition of unknown CPPS parameters, Acharya *et al.* have reconstructed the power system using publicly available data and have proposed a novel theoretical attack method to cause grid frequency instability by controlling the charging process of EVs [16]. Without knowledge of power system parameters, a coordinated EV switching attack has been launched to excite inter-area oscillations, resulting in grid destabilization [17]. Without relying on power system parameters, Soleymani *et al.* have proposed a data-driven load-altering attack leveraging EVs, which has led to notable

This work was supported by the Hong Kong Research Grant Council for the Research Project under Grant 15205424. *(Corresponding author: Siqi Bu.)*

Runzhuo Ma is with the Department of Electrical and Electronic Engineering, The Hong Kong Polytechnic University, Kowloon, Hong Kong SAR 999077, China (e-mail: runzhuo.ma@connect.polyu.hk).

Siqi Bu is with Department of Electrical and Electronic Engineering, Research Institute for Smart Energy, Policy Research Centre for Innovation and Technology, Research Centre for Grid Modernisation, and International Centre of Urban Energy Nexus, The Hong Kong Polytechnic University, Kowloon, Hong Kong SAR 999077, China, and also with the Shenzhen Research Institute, The Hong Kong Polytechnic University, Shenzhen, Guangdong 518000, China (e-mail: siqi.bu@polyu.edu.hk).

deviations in grid frequency and voltage [18]. However, these cyber-attacks have assumed that there are a sufficiently large number of controllable EVs at EVCSs and have not considered the driving flexibility of EVs.

Charging planning for EVs is usually executed by the EV charging navigation system (EVCNS), which analyzes both economic cost and time consumption to recommend the optimal EVCS for EV drivers [19]. The EVCNS relies on the communication network to efficiently transmit real-time transportation and charging data to the control center for globally optimized charging scheduling [20]. However, the connection of a large number of EVs not only increases grid load, but would also pose a potential threat to the secure operation of CPPSs [21]. Therefore, cybersecurity of EVs requires urgent attention to guard against possible systemic risks. Although many studies have been dedicated to optimizing charging planning strategies for EVs, they have not investigated the impact of cyber-attacks on EVCNS [22]. The vulnerability in the navigation communication network could provide an entry point for attackers to launch cyber-attacks.

Due to the high level of connectivity of CPPSs and CPTSs, a cyber-attack against CPTSs can indirectly threaten the secure operation of CPPSs. However, there are few studies that have focused on cyber-attacks against coupled systems. To fulfill this research gap and fully consider the vulnerability of vehicle navigation communication networks [23], this paper proposes a novel cyber-attack against EV charging planning. First, a two-level optimization model is constructed to identify the most vulnerable EVCS as a target for launching cyber-attacks when the CPPS parameters are unknown. Subsequently, cyber-attacks are designed to target the CPTS and EVCS charging price, respectively. By launching a joint cyber-attack, the planning results of EVCNS are altered. EVs will be attracted to the EVCS for charging, triggering operational failures in the CPPS and thus increasing the likelihood of cascading failures. The contributions of this paper can be summarized as follows.

(1). This paper proposes a novel joint cyber-attack against coupled power-transportation systems. The operational failure of the CPPS is induced by the cyber-attack launched against the CPTS, while ensuring that the cyber-attack remains undetected by both systems.

(2). A two-level analytical model is proposed to identify the most vulnerable EVCS as the attack target. The parameters required to construct the model are estimated from partially observable measurement data of CPPS, thereby enhancing the feasibility and accuracy of the cyber-attack.

(3). A successful cyber-attack can be executed at low cost, requiring only a small amount of data such as EVCS charging prices and traffic flow information. In addition, the attack vectors targeting the traffic flow are designed as sparse vectors to further reduce the attack cost.

The remaining sections of this paper are organized as follows. Section II presents the framework and process for launching the cyber-attack. The target EVCS identification scheme is developed in Section III. Section IV illustrates the design of cyber-attacks against EV charging route planning and charging price. The effectiveness of the proposed attack and its impact on the CPPS are verified in Section V. Finally, Section VI concludes this paper.

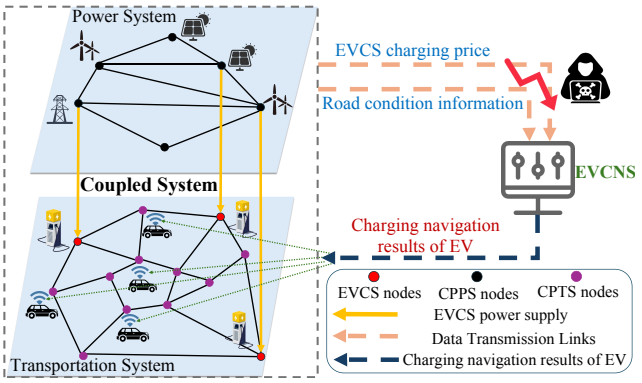


Fig. 1. Process of cyber-attacks against the EVCNS.

II. Cyber-attacks on Electric Vehicles Charging Navigation Systems

A. Overall Objectives of Charging Navigation Systems

When an EV initiates a charging request, road condition information and charging price will be transmitted to the EVCNS, which recommends the optimal EVCS for EV drivers. The optimal EVCS is usually determined in terms of both charging price and time consumption cost [24]. The overall objective of EVCNS at time t is modeled as shown in (1). EVCNS recommends an appropriate EVCS by minimizing $C(t)$ given driver preferences.

$$C(t) = \alpha P(t) + \beta \omega T(t) \tag{1}$$

where $C(t)$ is the total cost to reach the EVCS; $T(t)$ and $P(t)$ are the time consumption and financial cost to reach the EVCS, respectively; α and β are the weight factors, $\alpha+\beta = 1$; ω is the conversion coefficient for converting time to cost. Drivers will adjust α and β according to their preferences when choosing an EVCS.

Studies in recent years indicate that drivers commonly use navigation apps, and a large share of trips now rely on navigation systems [25]. It is worth noting that not all EV drivers use navigation apps for charging. The proposed cyber-attack targets EV drivers who use navigation apps and aims to enhance the attractiveness of the target EVCSs to draw sufficient EVs for a successful cyber-attack. The objective of the cyber-attack is not to attract all EVs to the target EVCSs.

B. Framework of Joint Cyber-Attack

The purpose of the cyber-attack is to increase the likelihood of cascading failures in CPPSs. According to Section II-A, to effectively attract EVs to the target EVCS, the attackers need to launch a joint cyber-attack to minimize the time consumption and financial cost for EVs at the target EVCS. This ensures that drivers are reasonably attracted to the target EV charging station regardless of their charging preferences. The overall process of the proposed cyber-attack are illustrated in Fig. 1.

TABLE I. DATA REQUIRED FOR THE CYBER-ATTACK

Data type	Action
CPPS measurement data	Estimate parameters and identify target EVCS
EVCS charging price	Launch cyber-attack against price signal
CPTS road condition data	Launch cyber-attack against route planning

C. Capabilities of Attackers

In this paper, a realistic distribution network is modeled as a partially observable CPPS with only 25% of the remote terminal units installed. In CPTSs, numerous sensors and monitoring devices ensure reliable operation [26]. The operational features of CPTSs and the widespread use of map software have generated vast publicly accessible data [27].

It is assumed that attackers can compromise the CPPS supervisory control and data acquisition network and collect a subset of measurement data [28]. The collected data can then be used for parameter estimation. Such data are typically obtained from remote terminal units and then transmitted to the supervisory control and data acquisition system. The parameter estimation can be completed prior to launching the cyber-attack.

On the other hand, the CPTS has integrated various advanced communication technologies, including the IEEE 1609 protocol for environmental monitoring and traffic flow analysis [29], as well as the Open Charge Point Protocol for transmitting price information [30], [31]. Attackers can leverage online device search engines such as Censys, Shodan, and Zoomeye to locate protocol backends, and exploit vulnerabilities such as cross-site scripting, cross-site request forgery, and structured query language injection, thereby launching cyber-attacks [18]. Attackers can continue launching attacks until a sufficient number of EVs are attracted. The simultaneous charging triggered by attackers can jeopardize the secure operation of the CPPS. Table I summarizes the types of data required for launching such cyber-attacks.

III. Identification of Target Electric Vehicle Charging Stations

In practical attack scenarios, limited resources and cost considerations make it difficult to coordinate simultaneous cyber-attacks across all EVCSs. However, targeting a single EVCS typically has only a limited impact. Therefore, this study focuses on analyzing cyber-attacks that target several EVCSs. Identifying the most critical combination of EVCSs is a prerequisite for launching an effective attack. In this section, We propose a method that integrates both attack cost and effectiveness to identify the target EVCS.

A. CPPS Parameter Estimation

The parameter estimation of the distribution network usually requires knowledge of the system state. Zhang *et al.* have successfully achieved accurate estimation of the dynamic distribution network topology and system state by employing a dirichlet-process hidden-markov model in conjunction with a particle filter algorithm [32]. This method requires only a small portion of the available measurement data. Inspired by this paper, attackers can use this approach to estimate the state of the distribution network when the parameters are unknown. It should be noted that this estimation method also requires pseudo-measurements of power injection at all buses (with a standard deviation of 20%).

In this section, multiple deep neural networks and error analysis methods are used to predict pseudo-measurements of power injection from limited data [33]. Specifically, three base learners and one meta learner are used during data training. The base learners are deep neural network models, and the meta learner uses random forest. Each base learner will generate its prediction result, and the results are compared by error analysis. The criterion is mean percentage error

$$MPE = \frac{1}{e}\sum_{i=1}^{e}\left|\frac{\hat{h}_i^m - h_i^m}{h_i^m}\right| \times 100\% \tag{2}$$

where h^m is the real measurement data, $\hat{h}^m$ is the estimated value, and e is the number of samples.

The mean percentage error values of each deep neural networks are compared, and the model with the smallest MPE is selected as the input to the meta learner, which is trained using a random forest algorithm. It is used to improve the prediction results and obtain more accurate pseudo-measurement values. This method requires only a few power flow measurements to generate accurate pseudo-measurements that fulfill the estimation requirements. This restores the CPPS to a fully observable system with state estimation. There are many ways to estimate the line parameters of the distribution network. Due to space constraints, the estimation process will not be described in detail here.

Based on the obtained CPPS parameters, attackers can simulate the power flow calculation of the CPPS. The power flow model can be represented as

$$P_i = v_i \sum_{j=1}^{n} v_j \left(G_{ij}\cos(\theta_i - \theta_j) + B_{ij}\sin(\theta_i - \theta_j)\right) \tag{3}$$

$$Q_i = v_i \sum_{j=1}^{n} v_j \left(G_{ij}\sin(\theta_i - \theta_j) - B_{ij}\cos(\theta_i - \theta_j)\right) \tag{4}$$

Let $M(\cdot)$ denote the process of power flow calculation. The branch power flow and node voltage based on the load z_{load} can then be expressed as

$$z_{\text{b}} = M(z_{\text{load}}), v_i = M(z_{\text{load}}) \tag{5}$$

B. Target EVCSs Identification for Joint Cyber-Attack

The initial contingency is defined as an outage or a combination of outages occurring within a short period of time, preventing effective corrective actions before the next event takes place [34]. Since the initial contingency plays a pivotal role in the initiation and propagation of cascading failures in CPPSs, identifying the initial contingency that may trigger potential cascading failures is essential for this study. This implies that attackers must target critical nodes of the CPPS to maximize the triggering potential and impact of an initial contingency. Accordingly, attackers can devise targeted cyber-attack strategies to activate these contingencies, thereby inducing cascading failures in the CPPS.

In this study, the proposed cyber-attack employs EVs as carriers, launching the attack by inducing load deviations. Such deviations typically lead to two adverse consequences: line overload and bus voltage violations. Furthermore, since CPPSs are generally equipped with $N-1$ contingency defense measures, the objective of such a cyber-attack is to induce a severe initial contingency that exceeds the $N-1$ defense capability. This includes the simultaneous tripping of multiple lines, voltage violations at several buses, or a combination of line overloads and bus voltage violations.

The condition for line overload tripping during CPPS operation are defined as follows.

$$|z_b|/z_{b,rate} \geq \Gamma \tag{6}$$

where $|z_b|$ represents the absolute value of the line power flow; $z_{b,rate}$ denotes the maximum rated capacity; Γ indicates per-unit overload threshold. In this study, Γ is set to 1.5.

During CPPS operation, bus voltages are typically maintained within specific thresholds to ensure system stability. The safety threshold range for bus voltage is defined as follows.

$$v_i^{min} < v_i < v_i^{max} \tag{7}$$

where v_i denotes the voltage of bus i; v_i^{min} and v_i^{max} represent the upper and lower safety thresholds for bus voltage, respectively. For this study, the lower and upper voltage thresholds are specified as 0.9 p.u. and 1.1 p.u., respectively.

In determining the combination of critical EVCSs, the analysis should not be limited to the CPPS alone but should also take the CPTS into account. Since the attack cost is generally constrained, attackers would typically aim to achieve the objective at the lowest possible cost. Therefore, when identifying vulnerable EVCSs, factors such as traffic flow and charging prices must also be considered, as these are important to ensure a reasonable attack budget.

Under known total charging costs, the charging decisions of EV drivers can be represented by the logit model, which captures the probabilistic nature of their choice behavior.

$$x_i = \frac{\exp(-C_{k,i})}{\sum_{j\in S}\exp(-C_{k,j})}, \quad \forall i \in S,\ \forall k \in K \tag{8}$$

where x_i denotes the probability of selecting EVCS i, and K represents the set of EVs.

For analytical convenience, we quantify the cost required to launch the cyber-attack. We assume that the attack cost is linearly related to the extent of data modification. Generally, the greater the amount of data that needs to be modified, the higher the expenditure required to achieve this objective. The attack cost is defined as follows.

$$C_{a,i} = \sum_{i\in\mathcal{S}} \left(c_i^p|\Delta p_i| + c_i^t|\Delta t_i|\right) \tag{9}$$

where $C_{a,i}$ denotes the total attack cost of EVCS i; $|\Delta p_i|$ and $|\Delta t_i|$ represent the amounts of data tampering in terms of price and time, respectively; c_i^p and c_i^t represent the corresponding unit costs.

The severity of initial contingencies caused by cyber-attacks differs among EVCS combinations. In addition, different types of faults exert different impacts on cascading failures in CPPSs. For attackers, an EVCS combination that produces a more severe effect and involves a lower cost is preferable. Therefore, a comprehensive assessment of cyber-attack effectiveness and associated costs is necessary to accurately identify the target EVCS combination.

A cyber-attack impact index for initial contingencies is defined, consisting of two components: the attack quantity effect $\mathcal{N}$ and the attack severity effect $\mathcal{H}$. The attack quantity effect is further measured by two factors: the number of overloaded lines and the number of buses with voltage violations.

$$\mathcal{N} = \omega_1^l \cdot \sum_i \mathcal{N}_l + \omega_1^v \cdot \sum_i \mathcal{N}_v, \forall i \in \bar{S} \tag{10}$$

where ω_1^l and ω_1^v denote the weight factors for line overloads and bus voltage violations, respectively; $\mathcal{N}_l$ and $\mathcal{N}_v$ are the numbers of overloaded lines and buses with voltage violations after the cyber-attack on EVCS i, respectively.

The attack severity effect is defined as follows:

$$\mathcal{H} = \omega_2^l \cdot \sum_{b\in O_i} \frac{\rho_b - \Gamma}{\Gamma} + \omega_2^v \cdot \sum_{e\in V_i} \frac{\delta v_e}{v_{\max} - v_{\min}}, \quad \forall i \in \bar{S} \tag{11}$$

where O_i and V_i are the sets of overloaded lines and buses with voltage violations after the cyber-attack; ρ_b and δv_e denote the load ratio and the voltage violation magnitude, respectively; and ω_2^l and ω_2^v are weight factors.

An attack impact index J to evaluate the attack impact is defined as follows:

$$J = \gamma_1 \frac{\mathcal{N}}{\mathcal{N}_{\max}} + \gamma_2 \frac{\mathcal{H}}{\mathcal{H}_{\max}} \tag{12}$$

where γ_1 and γ_2 are weight factors; $\mathcal{N}_{\max}$ and $\mathcal{H}_{\max}$ denote the maximum values across the EVCS combinations.

We formulate an optimization model to reallocate EV charging demand and trigger initial contingencies in the CPPS with minimal attack cost. The model identifies the optimal EVCS combination to increase the risk of cascading failures. Attackers select the target EVCSs by trading off attack cost against the attack impact index J.

$$\min_{\Delta p, \Delta t, s} \ \psi \cdot \mathcal{C} \ - \ (1-\psi)\cdot J \tag{13a}$$

$$\text{s.t.} \quad C_a = \sum_{i\in S} s_i \cdot \left(c_i^p\,|\Delta p_i| + c_i^t\,|\Delta t_i|\right) \tag{13b}$$

$$\mathcal{C} = C_a / C_{a,\max} \tag{13c}$$

$$C_{k,i} = (p_i^0 + \Delta p_i) + \omega\,(t_i^0 + \Delta t_i), \quad \forall k \in K,\ \forall i \in S \tag{13d}$$

$$x_{k,i} = \frac{\exp(-C_{k,i})}{\sum_{j\in S}\exp(-C_{k,j})}, \quad \forall k \in K, \forall i \in S \tag{13e}$$

$$\sum_{i\in S} x_{k,i} = 1, \quad x_{k,i} \geq 0, \quad \forall k \in K, \forall i \in S \tag{13f}$$

$$n_i^{req} \ = \ \sum_{k\in\mathcal{K}} x_{k,i}, \quad \forall i \in S \tag{13g}$$

$$n_i \ = \ s_j \cdot \min\{n_i^{ava},\, n_i^{req}\}, \quad \forall i \in S \tag{13h}$$

$$\Delta z_{\text{inj},e} = L \sum_{j\in S:\, b(j)=e} n_j\, \mathcal{A}_e, \quad \forall e \in E \tag{13i}$$

$$z_b' = M\big(z_{\text{load}} + \Delta z_{\text{load},i}\big), \quad \forall i \in E \tag{13j}$$

$$y_i^1 = \begin{cases} 1, & \text{if } \dfrac{|z_b'|}{z_{b,\text{rate}}} > \Gamma \\ 0, & \text{otherwise} \end{cases}, \quad \forall i \in B \tag{13k}$$

$$y_j^2 = \begin{cases} 1, & \text{if } v_i < v_{\min} \text{ or } v_i > v_{\max} \\ 0, & \text{otherwise} \end{cases}, \quad \forall j \in E \tag{13l}$$

$$\sum_j y_i^1 + \sum_i y_i^1 \geq 2, \quad \forall i \in B, \forall j \in E \tag{13m}$$

$$s_i \in \{0,1\}, \ \forall i \in S, \quad \bar{S} = \{\, i \in S \mid s_i = 1 \,\} \tag{13n}$$

$$\underline{\Delta p}_i \leq \Delta p_i \leq \overline{\Delta p}_i, \quad \forall i \in S \tag{13o}$$

$$\underline{\Delta t}_i \leq \Delta t_i \leq \overline{\Delta t}_i, \quad \forall i \in S \tag{13p}$$

$$c_i^p \geq 0, \quad c_i^t \geq 0, \quad \forall i \in S \tag{13q}$$

where $\underline{\Delta p}_i$ and $\overline{\Delta p}_i$ are the lower and upper bounds of price tampering, respectively; $\underline{\Delta t}_i$ and $\overline{\Delta t}_i$ are the lower and upper bounds of time tampering, respectively; $C_{a,\max}$ and $\mathcal{C}$ indicate the maximum attack cost and the normalized attack cost, respectively; p_i^0 and t_i^0 are the original price and time without attack; $C_{k,i}$ is the total cost to reach EVCS i; L and n denote the charging power of a single EV and the maximum capacity of the EVCS, respectively; n_i^{req} and n_i^{ava} indicate the number of attracted EVs and the number of available charging piles at EVCS i respectively; z_{b}' is the branch power flow after the load change; $\Delta z_{load,i}$ denotes the increase in power injected into the bus i; $\mathcal{A}$ is a diagonal matrix with binary entries $\mathcal{A}_i \in \{0,1\}$, where $\mathcal{A}_i = 1$ if the load is increased at bus i and $\mathcal{A}_i = 0$ otherwise; B and E denote the branch and node sets, respectively; S and $\bar{S}$ indicate the set of all EVCSs and the set of attacked EVCSs, respectively. The solution method for this model is detailed in Appendix A.

IV. Design of Joint Cyber-Attack

A. Objective of Cyber-Attack on Route Planning

The cyber-attack against route planning is essentially an attack on $T(t)$. Specifically, $T(t)$ can be expressed as [22].

$$T(t) = T_d(t) + T_w(t) + T_c(t) \tag{14}$$

where $T_d(t)$ is the driving time of the EV to the target EVCS at the time t, $T_w(t)$ is the waiting time at the target EVCS, and $T_c(t)$ is the charging time.

In real CPTSs, traffic flow varies throughout the day. Dynamic road congestion not only affects the route planning for EVs but can also alter the optimal selection of the EVCS. The transportation network can be modeled as an undirected graph $\mathcal{G} = (\mathcal{I}, \mathcal{R})$, where $\mathcal{R}$ denotes roads, and $\mathcal{I}$ represents intersections. In CPTSs, dynamic road congestion can be reflected in driving time, where driving time through a road is modeled as the latency function [35].

$$t_{uv}(\eta_{uv}(t)) = \left(\frac{\mathcal{D}_{uv}}{s_{uv}}\right)\left[1 + 0.15\left(\frac{\eta_{uv}(t)}{c_{uv}}\right)^4\right], u, v \in I \tag{15}$$

where $\eta_{uv}(t)$ indicates the traffic flow of $\mathcal{R}_{uv}$ at time t; t_{uv} is the driving time of $\mathcal{R}_{uv}$; c_{uv} represents the capacity of $\mathcal{R}_{uv}$; $\mathcal{D}_{uv}$ denotes the length of R_{uv}; s_{uv} is the speed limit of $\mathcal{R}_{uv}$.

The total driving time to the EVCS can be calculated as:

$$T_d(t) = \sum_{\mathcal{R}_{uv} \in R} t_{uv} \tag{16}$$

The driving route can be represented as:

$$R = \mathcal{R}_{uj} \rightarrow \mathcal{R}_{jv} \rightarrow \cdots \rightarrow EVCS \tag{17}$$

The waiting time refers to the period when an EV arrives at the EVCS and waits in line for charging. Attackers can compromise Open Charge Point Protocol to tamper with the status of charge piles at the target EVCSs, creating the illusion that those EVCSs always have charging piles available. Therefore, regardless of the modeling approach, $T_w(t)$ is assumed to be zero. The charging time can be expressed as:

$$T_c(t) = \frac{E_T - E_I}{P_{charge}} \tag{18}$$

where P_{charge} is the charging rate of EVs; E_T and E_I denote the target and initial power levels of the charging EVs. Since the energy consumption of EVs driving to an EVCS is small and usually negligible [36], all EVs at different EVCSs have the same charging time T_c. Therefore, the target of time based cyber-attack is the driving time.

In the EVCNS, route planning aims to identify the EVCS with the shortest total time for EV charging and plan the driving route. The centralized approach is commonly used in the EVCNS, with route planning typically based on the Dijkstra algorithm [37].

B. Demand-Price Relationship for EV Charging at EVCSs

The cyber-attack against financial cost targets $P(t)$ at the target EVCS. Since the energy consumption of EVs driving to an EVCS is negligible, the financial cost is only attributed to EV charging. Therefore, $P(t)$ can be represented as:

$$P(t) = P_c(t) = p_i(t) \cdot (E_T - E_I) \tag{19}$$

Hence, the cyber-attack against financial cost is equivalent to manipulating the charging price of EVCS. The EVCS operator determines the charging price based on a combination of factors such as distribution locational marginal price and profitability of EVCSs. Competition exists among different EVCSs, and price-sensitive EV drivers typically select their target EVCS based on the charging price.

In economic theory, demand and price are inversely related. Moreover, the relationship between EV charging demand and charging price is nonlinear. Therefore, an exponential distribution is used in (20) to model the relationship between the probability of demand and the charging price between two EVCSs [38].

$$Pr_i = \rho_t^{i,j} e^{\rho_t^{i,j} p_j(t)}, \quad \forall j \in S, i \neq j \tag{20}$$

where $\rho_t^{i,j}$ is a coefficient describes the relationship between the probability of demand and the charging price of ith EVCS.

Extending the model to multiple EVCSs, the probability of EV reaching the target EVCS is $Pr_{N_t^j}$. The EV demand for the ith EVCS can be represented as:

$$N_t^i = Pr_{N_t^i} \cdot N_t \tag{21}$$

where N_t^j indicates the demand for EVs attracted by the ith EVCS; N_t is the EV demand that need to select EVCS at t. The derivation processes of $\rho_t^{i,j}$ and $Pr_{N_t^i}$ are outlined in Appendix B and C, respectively.

C. Construction of Joint Cyber-Attack

1) Construction of Cyber-Attack against Route Planning

As analyzed in Section IV-A, the cyber-attack on route planning essentially targets T_d. By falsifying the measurement data in CPTS, the driving time to target EVCSs can be minimized. Since $\mathcal{D}_{uv}$, s_{uv} and c_{uv} are predetermined after road construction and are typically regarded as fixed values, the traffic flow data are regarded as manipulable data. Considering both stealth and attack cost, the optimization aims to minimize the number of data points to be modified while ensuring the success of the attack. The cyber-attack model for route planning is shown in (22).

$$\min f = [f_1, f_2] \tag{22a}$$

$$\text{s.t.} \quad f_1 = t_{att}^i / t_{att}^{\min} \leq 0.8, \quad f_2 = \left\| z^T - z_{att}^T \right\|_0, \forall i \in \bar{S} \tag{22b}$$

$$z_{att,\min}^T \leq z_{att}^T \leq z_{att,\max}^T \tag{22c}$$

$$\mu - \pi\sigma \leq z_{att}^T \leq \mu + \pi\sigma \tag{22d}$$

$$\sum_{k \in S} \phi_k = 1 \tag{22e}$$

$$\sum_{i,j} \mathcal{R}_{ij} - \sum_{i,j} \mathcal{R}_{ji} = \begin{cases} 1 & \text{if } i \in (\mathcal{I} - S), \\ 0 & \text{if } i \notin (\mathcal{I} - S),\ i \notin S \\ -\phi_i & \text{if } i \in S \end{cases} \tag{22f}$$

where t_{att}^i is the driving time of the EV to target EVCSs after attack; t_{att}^{min} is the shortest time consumption of the remaining EVCSs after target EVCSs is excluded; z^T and z_{att}^T are the measurement data before and after the cyber-attack, respectively; μ and σ are the mean and standard deviation, which can be obtained from historical data. $\pi = 3$ indicates 3σ method for outlier detection; $\|\bullet\|_0$ indicates the L0-norm.

An adaptive multi-objective particle swarm optimization algorithm incorporating a dynamic reference vector mechanism and a hybrid archiving strategy is proposed to solve the problem. The algorithm utilizes dynamic reference vector to automatically track the pareto front and employs a two-stage archive update strategy that integrates ϵ-dominance-based fast-filtering and dynamic reference vector-guided fine selection, thereby maintaining solution diversity while reducing computational cost. In addition, objective-specific mutation and crossover operations are designed based on specific optimization goals. Through adaptive control mechanisms, the algorithm prevents premature convergence and enhances solution quality. The sub-algorithms are provided in Appendix D.

2) Construction of Cyber-Attack Against Charging Price

In this section, an adaptive cyber-attack scheme on the charging price is designed to dynamically modify the price based on the load data of EVCSs. The purpose is to ensure that the charging price of target EVCSs remain the lowest among all EVCSs during the attack period. The attack amplitude ($\delta(t)$) for the charging price is designed as follows.

$$\delta(t) = \left(p_i^*(t) - \min_{j \neq i} p_j^*(t) + \epsilon \right) \cdot \kappa(t) \tag{23}$$

where $p_i^*(t)$ indicates the charging price of target EVCSs; $\kappa(t)$ is an adaptive factor to control the attack magnitude.

During the course of the attack, charging prices may fluctuate due to a variety of factors. Therefore, a dynamic attack signal is designed, where the attack amplitude is dynamically adjusted based on the number of EVs attracted to target EVCSs. $\delta(t)$ can adaptively respond to different competitive environments. The goal is to attract more EV drivers by reducing prices, while avoiding excessive price reductions that could raise suspicion.

In addition, to ensure the stealthiness of the cyber-attack, attackers should maintain reasonable fluctuations in the price signal. Attack prices can be formulated based on the historical price distribution so that the attack can avoid generating outliers that can be easily detected. The model of the cyber-attack against charging price is shown below.

$$\min \quad p_i(t), \forall t \in T, \forall i \in \bar{S} \tag{24a}$$

$$\text{s.t.} \quad p_i(t) = p_i^*(t) - \delta(t), \forall t \in T, \forall i \in \bar{S} \tag{24b}$$

$$\delta_{min} \leq \delta(t) \leq \delta_{max}, \forall t \in T \tag{24c}$$

$$\delta(t) = \left(p_i^*(t) - \min_{j \neq i} p_j^*(t) + \epsilon \right) \cdot \kappa(t), \forall t \in T, \forall i \in \bar{S} \tag{24d}$$

$$\kappa(t) = k \cdot \left(\mathcal{E} \cdot \frac{N_t^i}{N_t} + (1 - \mathcal{E}) \right), \forall t \in T, \forall i \in \bar{S} \tag{24e}$$

$$Pr_{N_t^j} = \rho_t^{i,j} e^{\rho_t^{i,j} p_j(t)}, \quad \forall j \in S \tag{24f}$$

Algorithm 1 Dynamic Reference Vector-Adaptive Multi-Objective Particle Swarm Optimization

Input:Population size N, max iteration T, objectives f_1, f_2
Output: Non-dominated archive A
Require: Algorithm 2, 3, 4
Initialize:
  $P \leftarrow$ Random population of N particles
  $V \leftarrow$ DynamicReferenceVectors
  $A \leftarrow \emptyset$
  updater $\leftarrow$ ParticleUpdater$(w_{\min}, w_{\max})$
for $t = 1$ to T
  V.adapt_vectors(A)
  $\mathbf{g_i^{best}} \leftarrow V$.assign_solutions$(A)$
  for $i = 1$ to N **do**
    $w_i, P[i] \leftarrow$ updater.update_particle$(P[i], A)$
    $\mathbf{v}_i \leftarrow w_i \mathbf{v}_i + c_1 r_1 (\mathbf{p_i^{best}} - \mathbf{x}_i) + c_2 r_2 (A[\mathbf{g_i^{best}}] - \mathbf{x}_i)$
    $\mathbf{x}_i \leftarrow \mathbf{x}_i + \mathbf{v}_i$
    if rand() $< P_{\text{crossover}}$ **then**
      $\mathbf{x}_i \leftarrow$ ratio_aware_crossover$(\mathbf{x}_i, A, f_1)$
    end if
  end for
  $A \leftarrow$ ArchiveManager.update$(P \cup A, V$.vectors$)$
end for
return A

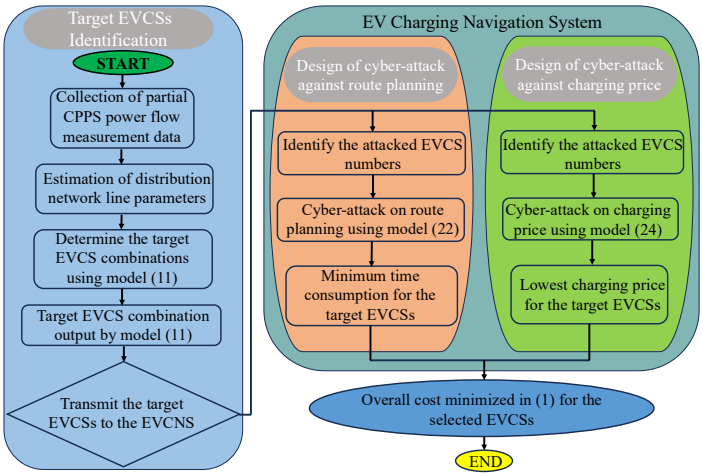


Fig. 2. Overall framework of the joint cyber-attack.

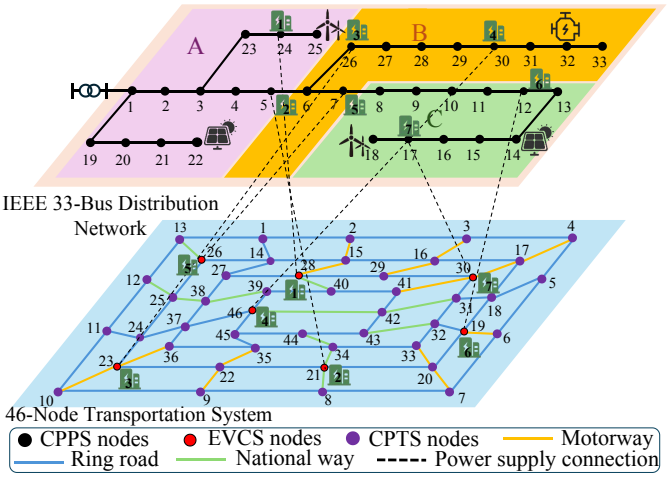


Fig. 4. Structure of the test coupled system.

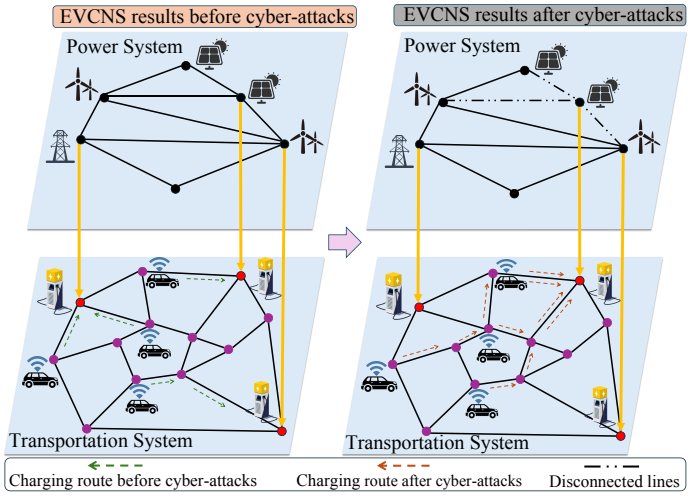


Fig. 3. Consequences of the joint cyber-attacks.

$$p_j(t) = \begin{cases} p_i(t), & j = i \\ p_j^*(t), & j \neq i \end{cases}, \forall j \in S, \forall t \in T, \forall i \in \bar{S} \quad (24g)$$

$$N_t^j = \left(N_t \cdot Pr_{N_t^j}\right) \geq 0, \forall j \in S, \forall t \in T \quad (24h)$$

$$p_i(t) \leq \min_{j \neq i} p_j^*(t) - \epsilon_p, \forall t \in T, \forall i \in \bar{S} \quad (24i)$$

$$\mu_p - \gamma \sigma_p \leq p_i(t) \leq \mu_p + \gamma \sigma_p, \forall t \in T, \forall i \in \bar{S} \quad (24j)$$

where $p_i^*(t)$ and $p_i(t)$ are the charging price of target EVCSs before and after the cyber-attack, respectively; $p_j^*(t)$ is the charging price of other EVCSs; μ_p, σ_p and γ_p are the mean, standard deviation, and tolerance coefficient of the price distribution; ϵ and ϵ_p are smaller fixed values; k is the attack strength scaling factor to control the overall strength of the attack amplitude; $\mathcal{E}$ is a weight factor; N_t and N_t^j indicate the total EV charging demand and the number of EVs that choose EVCS i for charging, respectively. The derivation processes of k are outlined in Appendix E.

The cyber-attack framework and results are presented in Figs. 2 and 3, respectively.

V. Case Study

A. Simulation Setup

In this section, a coupled system containing an IEEE 33-bus distribution network and a 46-node transportation system is used to verify the effectiveness of the proposed cyber-attack. The CPTS is adapted from the real transportation network [39], and the data for the CPTS is shown in [40]. The CPPS data are obtained from the Matpower 7.1 toolbox. The topology of the coupled system is shown in Fig. 4.

The CPPS contains several distributed generators, with wind turbines at nodes 14 and 22, photovoltaics at nodes 18 and 25, and a diesel generator at node 32. The wind turbines and photovoltaics have capacities of up to 400 kW, while the diesel generator has a capacity of up to 1,000 kW. It is assumed that intelligent attackers launch cyber-attacks during periods of high load in the CPPS. To simulate the peak load condition, the load is set to increase by a factor of 1.2 in Zone A, 1.25 in Zone B, and 1.35 in Zone C.

B. Results of Target EVCSs Identification

Since the CPPS parameters are necessary for attackers to determine target EVCSs, they are first estimated. The relative error is used to verify the accuracy of parameter estimation. The estimation results are shown in Fig. 5. The results show that errors in the estimation of branch conductance and susceptance based on partial data are less than 1%. This indicates that line parameters can be accurately estimated under partially observable conditions [41].

Before the cyber-attack is executed, attackers infiltrate in the cyber layer of CPPS to obtain measurement data and identify the target EVCSs by the EVCS identification model. It is assumed that each EVCS has 20 charging piles and the charging power of each pile is 150 KW. During the cascading failure propagation process in CPPSs, line overloads generally exert a more critical impact than voltage violations. The tripping of overloaded lines alters the topology of the CPPS, which can substantially increase the probability of subsequent cascading outages. To appropriately capture this characteristic, the weighting parameters of $\mathcal{N}$ are set to $\omega_1^l = 2$ and $\omega_1^v = 1$,

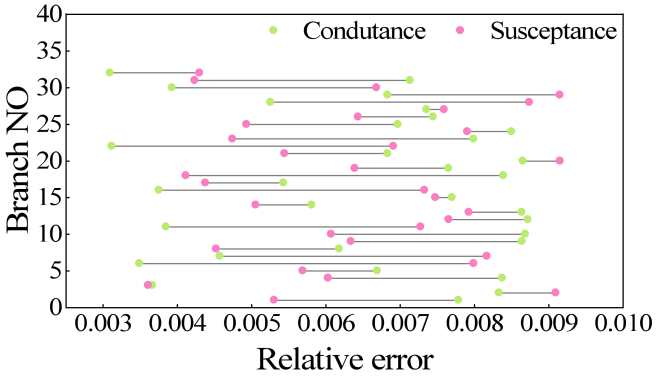


Fig. 5. Line parameters estimation errors.

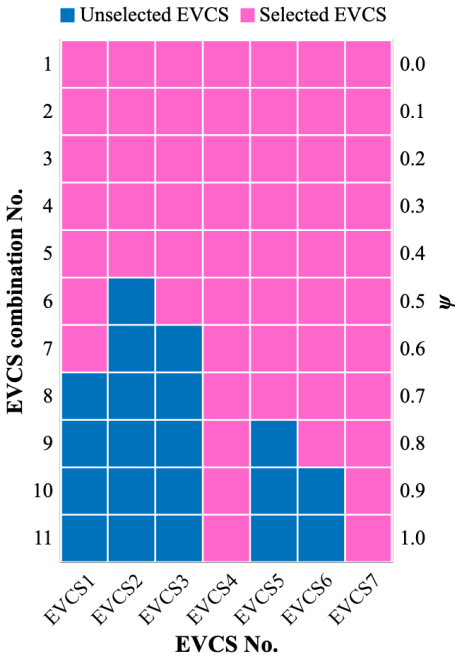


Fig. 6. Target EVCS combinations for different values of ψ.

thereby prioritizing EVCS combinations that lead to a higher number of overloaded lines.

In addition, the weight coefficients $\omega_2^l = 2$ and $\omega_2^v = 1$ used in constructing $\mathcal{H}$ are assigned in the same manner. This choice biases the evaluation toward combinations that cause the most severe overloads, reflecting the dominant role of line tripping in initiating and propagating cascading failures. It also keeps the analysis consistent with practical system behavior, where overload induced contingencies are typically more disruptive to stability than voltage limit violations. Moreover, when evaluating attack impact, fault count has greater influence on CPPS cascading failures than fault severity. Accordingly, the weight factors γ_1 and γ_2 are set to 0.6 and 0.4, respectively.

We vary the weight ψ from 0 to 1 in steps of 0.1 to examine the outputs of the target EVCS identification model. Since ψ reflects the attack preference, the resulting set of target EVCSs may differ across weights. The identified combinations at different weights are shown in Fig. 6, and the consequences of cyber-attacks on different combinations of EVCSs are summarized in Table II.

TABLE II. CONSEQUENCES OF CYBER-ATTACKS ON DIFFERENT EVCS COMBINATIONS

EVCS Combination No.	Severe Overload Lines	Bus Voltage Violation
1	1-2,2-3,3-4,4-5,5-6, 7-8,8-9,3-23,23-24,6-26	6,7,...,18, 26,27,...,33
2	1-2,2-3,3-4,4-5,5-6, 7-8,8-9,3-23,23-24,6-26	6,7,...,18, 26,27,...,33
3	1-2,2-3,3-4,4-5,5-6, 7-8,8-9,3-23,23-24,6-26	6,7,...,18, 26,27,...,33
4	1-2,2-3,3-4,4-5,5-6, 7-8,8-9,3-23,23-24,6-26	6,7,...,18, 26,27,...,33
5	1-2,2-3,3-4,4-5,5-6, 7-8,8-9,3-23,23-24,6-26	6,7,...,18, 26,27,...,33
6	1-2,2-3,3-4,4-5,5-6, 7-8,8-9,3-23,23-24,6-26	7,8,...,18, 27,28,...,33
7	1-2,2-3,3-4,4-5,5-6, 7-8,8-9,3-23,23-24	8,9,...,18, 28,29,...,32
8	1-2,2-3,3-4,4-5,5-6, 7-8,8-9	8,9,...,18, 29,30,31
9	1-2,2-3,4-5,5-6, 7-8,8-9	8,9,...,18
10	4-5	9,10...,18
11	4-5	9,10...,18

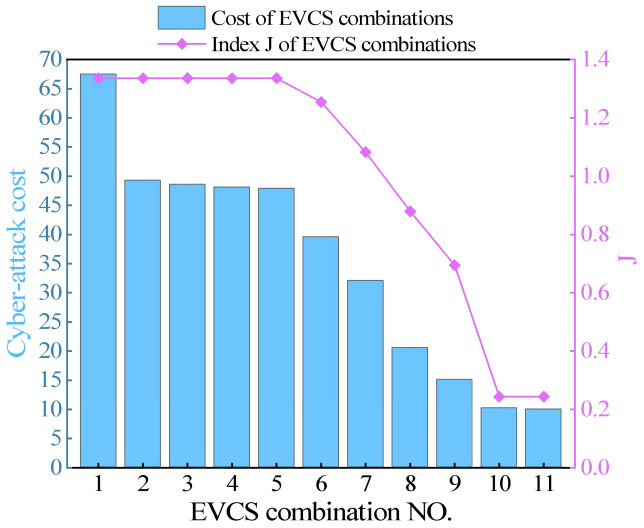


Fig. 7. Comparison of attack cost C and impact index J for different EVCS combinations.

As shown in Fig. 6, the identified EVCS set remains unchanged for $\psi \in [0, 0.4]$. When ψ is small, the objective places greater emphasis on attack impact J, so the high-impact combination stays optimal. At $\psi = 0.5$, the weights on attack cost C and attack impact J are balanced. The model begins to trade off between the two and the target EVCS set changes for the first time. As ψ increases further, the model prioritizes economic efficiency and reduces the number of EVCS in the target set to decrease the attack cost. Consistent with Table II, for $\psi \in [0.5, 0.9]$ the achievable attack impact gradually declines as the weight on cost increases. Once ψ reaches 0.9, the target set shrinks to two EVCSs. Given the minimum attack impact constraint (13m), the selection no longer changes beyond this point. Even for larger ψ, the identified target set remains the same as at $\psi = 0.9$.

Assume attackers seek to achieve a successful cyber-attack at the lowest feasible cost while maximizing impact and satisfying the minimum impact requirement. Fig. 7 compares attack cost with the impact index J for each EVCS combination. Since combination 1 ($\psi = 0$) ignores the cost term, the optimizer pushes $|\Delta p|$ and $|\Delta t|$ to their bounds to maximize impact. Therefore this combination has the highest cost. When $0 < \psi < 0.5$, attackers begin to account for attack cost and trade off cost and impact, but the impact term still dominates the objective. As a result, these combinations select the same EVCS set and their costs are similar. Combinations 1 to 5 yield the highest J. Their costs are prohibitive and unattractive for resource-constrained attackers. Combinations 10 to 11 are the cheapest and only just meet the minimum impact threshold. Each produces only one overloaded line. Moreover, brief operation outside the voltage limits is typically tolerable for the CPPS. Therefore the operational stress is limited. Combinations 6 to 9 strike a balance between cost and impact. Among them, combination 9 increases cost only slightly relative to 10 to 11. It delivers a much larger impact and causes multiple line overloads. This raises the risk of cascading failure propagation. Therefore the selected target combination is No. 9. It corresponds to EVCS 4, 6, and 7.

C. Performance of the Joint Cyber-Attacks

Once the target combination of EVCS is identified, attackers can launch cyber-attacks against these EVCSs accordingly. Since the attack methodology is identical across multiple EVCSs, EVCS 4 is selected as a representative case for the evaluation of the effectiveness of the proposed cyber-attack.

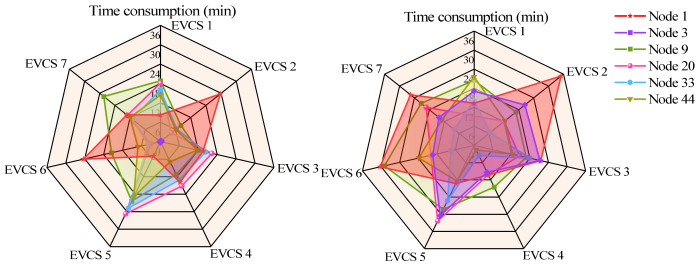
1) Performance of the Cyber-Attacks on Route Planning

There are different types of roads in the CPTS, each associated with data such as speed limits. These roads can be classified as motorways, ring roads, and national highways [39]. By falsifying traffic flow data within the normal range so that the values do not appear as outliers, the attackers can ensure that the driving time to the target EVCS is shortest.

In this part, EVCS 4 is selected as the target to evaluate the impact of the cyber-attack on route planning. To preserve generality, several locations in the CPTS are randomly chosen. It is assumed that EVs initiate charging requests from nodes 1, 3, 9, 20, 33, and 44. The EVCNS will calculate the time consumption of each EV to reach its optimal EVCS. Fig. 8 presents the time consumption for the EVs to reach each optimal EVCS before and after the cyber-attack.

It can be seen that under normal conditions, the EVCSs recommended for EVs at nodes 1, 3, 9, 20, 33, and 44 are EVCS 5, 7, 2, 6, 6, and 2, respectively. Notably, EVCS 4 is not selected as the optimal EVCS for any of these EVs. The route planning results are summarized in Table IV.

When EVCS 4 is attacked, all EVs exhibit the shortest driving time to EVCS 4. As a result, EVCS 4 is identified as the optimal EVCS during the route planning process, thereby fulfilling the objective of the cyber-attack. In conjunction with Fig. 4, it can be observed that under normal circumstances, the EVCNS typically recommends the nearest EVCS to drivers. However, during the cyber-attack period, attackers falsify real-time traffic flow data from the CPTS, creating artificial congestion on roads. This significantly increases the driving time to the originally recommended EVCSs, thereby misleading the EVCNS and influencing its route planning decisions. Table V presents the route planning results and the driving times of the EVs to reach the target EVCS after the cyber-attack. This confirms the successful execution of the attack on $T(t)$ in (1).



(a). Before cyber-attacks (b). After cyber-attacks

Fig. 8. Comparison of driving time to reach each EVCS before and after cyber-attacks.

TABLE III. ROUTE PLANNING AND TIME CONSUMPTION WITHOUT CYBER-ATTACK

Location of EV in CPTS	EVCS Recommendation	Optimal Routing	Time Consumption
1	5	$1 \rightarrow 14 \rightarrow 26$	5.03 min
3	7	$3 \rightarrow 16 \rightarrow 29 \rightarrow 30$	6.26 min
9	2	$9 \rightarrow 22 \rightarrow 21$	8.07 min
20	6	$20 \rightarrow 19$	3.13 min
33	6	$33 \rightarrow 32 \rightarrow 19$	3.95 min
44	2	$44 \rightarrow 34 \rightarrow 21$	6.07 min

TABLE IV. ROUTE PLANNING AND TIME CONSUMPTION WITH CYBER-ATTACK

Location of EV in CPTS	EVCS Recommendation	Optimal Routing	Time Consumption
1	4	$1 \rightarrow 14 \rightarrow 27 \rightarrow 38 \rightarrow 39 \rightarrow 46$	10.36 min
3	4	$3 \rightarrow 4 \rightarrow 5 \rightarrow 18 \rightarrow 31 \rightarrow 32 \rightarrow 46$	9.41 min
9	4	$9 \rightarrow 22 \rightarrow 35 \rightarrow 36 \rightarrow 37 \rightarrow 46$	4.92 min
20	4	$20 \rightarrow 33 \rightarrow 34 \rightarrow 44 \rightarrow 45 \rightarrow 46$	10.27 min
33	4	$33 \rightarrow 34 \rightarrow 44 \rightarrow 45 \rightarrow 46$	3.53 min
44	4	$44 \rightarrow 45 \rightarrow 46$	1.53 min

2) Performance of Cyber-Attacks on Charging Price

Based on the previous analysis, EVCS 4 is selected as the target EVCS. The attackers aim to falsify measurement data so that the charging price of EVCS 4 becomes the lowest among all EVCSs. A cyber-attack targeting charging prices is analyzed over 20 discrete time steps. Fig. 9 illustrates the distribution of charging prices for all EVCSs before and after the cyber-attack. It can be seen that the charging prices of all EVCSs vary and fluctuate under normal conditions, and EVCS 4 does not consistently offer the lowest price. However, during the cyber-attack, the charging price of EVCS 4 is consistently manipulated to remain the lowest throughout the attack duration.

The magnitude of the attack signal is adaptively adjusted

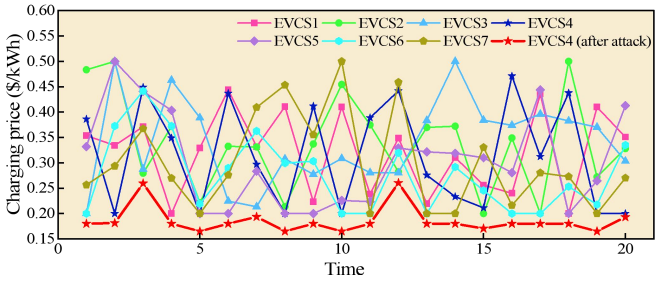


Fig. 9. Charging price comparison between normal conditions and cyber-attack on EVCS 4.

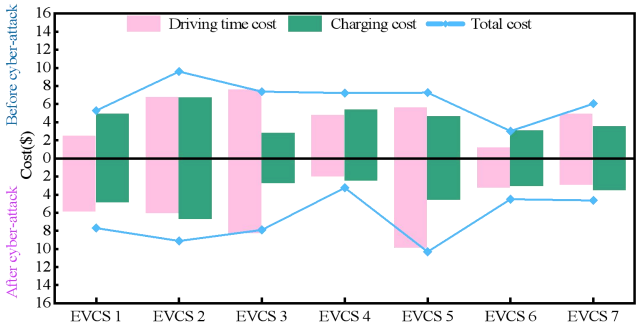


Fig. 10. Comparison of total, charging, and time costs for EVCSs before and after the joint cyber-attack.

based on the charging demand at the target EVCS, allowing it to dynamically change under varying load conditions. This design fulfills the attack purpose while making the price change reasonable. It can also be observed from Fig. 9 that the charging price of EVCS 4 after the attack is not excessively different from the lowest price of the remaining EVCSs, thereby reducing the likelihood of detection and suspicion. In addition, the cyber-attack is launched solely on the target EVCS, with the prices of other EVCSs remaining unchanged, which further enhances the stealthiness of the attack. For price-sensitive EV drivers, such an attack can plausibly attract them to the target EVCS, thereby realizing the attack on $P(t)$.

3) EVCS Recommendation Results

Combining the cyber-attack against charging price with the cyber-attack against driving time can effectively and strategically attract EVs to the target EVCS, thereby disrupting the secure operation of CPPSs. Taking an EV that initiates a charging request at node 30 in the CPTS with a charging demand of 100 kWh as an example, Fig. 10 compares the total cost, charging cost, and driving time cost of each EVCS before and after the cyber-attack.

Under normal conditions, the EVCNS recommends the EVCS with the lowest total cost to the driver by considering both price and time information. As illustrated in Fig. 10, when considering both charging price and time cost, EVCS 6 is the optimal choice. If the charging preference of the driver focuses on time, EVCS 6 would be recommended; if it focuses on charging price, EVCS 3 would be preferred. However, after the joint cyber-attack is launched, EVCS 4 becomes the most attractive choice, as both its charging price and driving time are minimized.

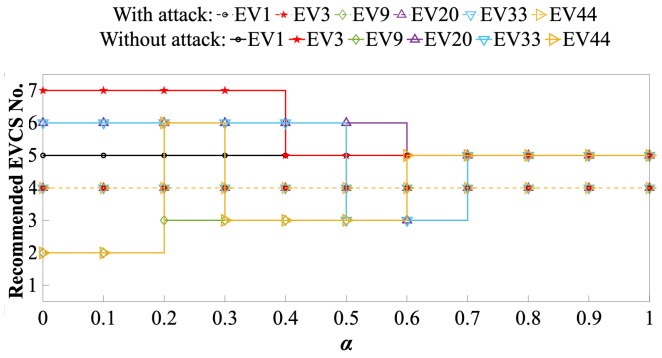


Fig. 11. Comparison of EVCS recommendation sensitivity to preference parameter with and without the cyber-attack.

We again consider EVs at CPTS positions 1, 3, 9, 20, 33 and 44, denoted EV 1, EV 3, EV 9, EV 20, EV 33, and EV 44, to analyze preference parameter sensitivity. The parameter α is varied over $[0, 1]$ in steps of 0.1. Since $\beta = 1 - \alpha$, a complete sweep of α is equivalent to a sweep of β. Therefore, the sensitivity analysis is conducted only with respect to α, without separately evaluating β. Given the coefficient ω, the total cost of each EVCS is computed by (1).

Fig. 11 compares the EVCS recommendation results for EVs at different locations, under varying α, in the presence and absence of the cyber-attack. Without cyber-attacks, EVCS recommendations exhibit stepwise changes with different α, reflecting normal sensitivity to driver preferences. Across the entire range, EV 1 is consistently assigned to EVCS 5 regardless of preference. For EV 3, the recommendation switches from EVCS 7 to EVCS 5 as α increases. By contrast, the recommendations for EV 9, EV 20, EV 33, and EV 44 switch multiple times among EVCS 2, 3, 5, and 6 as α changes. Notably, EVCS 4 is not selected for these EVs under any parameter settings. Under the cyber-attack scenario, EVCS 4 has the lowest charging cost and time consumption, leading to the lowest comprehensive cost for all α. As a result, the recommendations lose sensitivity to preferences and remain locked. Consequently, regardless of driver preferences, the EVCNS uniformly recommends EVCS 4 for these EV drivers.

D. Countermeasures Against the Cyber-Attack

This study designs a novel cyber-attack model to draw attention to potential risks in CPPS operations. On the defensive side, practical strategies are suggested to enhance detection capability against such threats. Future research will advance this work through detailed quantitative evaluation and the design of more sophisticated defense algorithms.

In EVCSs, charging prices are typically determined based on distribution locational marginal prices. Under normal conditions, charging prices align closely with the corresponding distribution locational marginal prices. If the price at a given bus is high, the charging price at the EVCS connected to that bus will also be high, whereas if the price is low, the corresponding charging price will be low. Consequently, once charging prices are tampered with, the correspondence between charging prices and distribution locational marginal

prices will deviate. By continuously comparing charging prices at EVCS with the associated nodal distribution locational marginal prices, operators can effectively detect such manipulation.

For driving time manipulation attacks, the adversary must continuously compromise the communication channel to maintain falsified traffic flow information. To mitigate this risk, operators can periodically inspect the security of communication channels and employ encrypted data transmission to prevent unauthorized modification. In addition, an intrusion detection system can be integrated into the EVCNS to identify abnormal recommendation patterns. For example, if a particular EVCS persistently appears as the shortest driving time option for EVs departing from diverse locations, this may indicate that the underlying driving time data has been maliciously manipulated.

VI. Conclusion

This paper proposes a novel cyber-attack strategy targeting coupled power–transportation systems. By exploiting partial observational data, attackers can identify target EVCSs. They can then jointly manipulate charging prices and driving times to covertly and reasonably attract EVs to these EVCSs, thereby threatening the secure operation of CPPSs. This study not only reveals a potential cross-domain cyber-attack approach and highlights the risks such cyber-attacks pose to power systems, but also provides insights into strengthening the resilience of integrated power–transportation systems. However, this study focuses primarily on fast-charging station scenarios, while the current level of deployment remains relatively limited. In addition, parameter estimation is required to identify target EVCSs. These factors constitute the limitations of this study. Future research will aim to estimate CPPS parameters using fewer measurements or determine target EVCSs without relying on CPPS parameters. The scope will also be extended to more complex coordinated power–transportation cyber-attack scenarios and their corresponding defense strategies.

Appendix

A. Solution Process for the Target EVCSs Identification Model

1) Attack cost linearization

For the EVCS identification model, constraint (13b) contains absolute value terms, we introduce two non-negative variables u_i^p and u_i^t, defined as follows:

$$u_i^p \geq |\Delta p_i|, \quad u_i^p \geq 0, \quad \forall j \in S \tag{25}$$

$$u_i^t \geq |\Delta t_i|, \quad u_i^t \geq 0, \quad \forall i \in S \tag{26}$$

Under minimization, (25) and (26) yield $u_i^p = |\Delta p_i|$, $u_i^t = |\Delta t_i|$. We define

$$w_i^p = s_i\, u_i^p, \quad w_i^t = s_i\, u_i^t, \quad s_i \in \{0,1\}, \quad \forall i \in S \tag{27}$$

Let $U_i^p = \max\{|\underline{\Delta p}_i|, |\overline{\Delta p}_i|\}$, $U_i^t = \max\{|\underline{\Delta t}_i|, |\overline{\Delta t}_i|\}$. Then (27) is equivalently enforced by the following constraints

$$0 \leq w_i^p \leq U_i^p\, s_i \quad \forall i \in S \tag{28}$$

$$w_i^p \geq u_i^p - U_i^p\,(1 - s_i), \quad \forall i \in S \tag{29}$$

$$0 \leq w_i^t \leq U_i^t\, s_i \quad \forall i \in S \tag{30}$$

$$w_i^t \geq u_i^t - U_i^t\,(1 - s_i), \quad \forall i \in S \tag{31}$$

The attack cost can be converted as follows

$$C_a = \sum_{i \in \mathcal{S}} \left(c_i^p\, w_i^p + c_i^t\, w_i^t\right) \tag{32}$$

2) Convex-equivalent derivation of the logit model

The logit model in (13e) is nonconvex. To obtain a convex formulation, define

$$Z_k = \sum_{j \in S} e^{-C_{k,j}}, \qquad q_{k,i} = \frac{e^{-C_{k,i}}}{Z_k} \tag{33}$$

By Gibbs inequality (the log-sum inequality), for any probability vectors x_k and q_k,

$$\mathrm{KL}(x_k \,\|\, q_k) = \sum_i x_{k,i} \ln \frac{x_{k,i}}{q_{k,i}} \geq 0 \tag{34}$$

with equality iff $x_k = q_k$. Using $\ln q_{k,i} = -C_{k,i} - \ln Z_k$,

$$\begin{aligned} \mathrm{KL}(x_k \| q_k) &= \sum_i x_{k,i} \ln x_{k,i} - \sum_i x_{k,i} \ln q_{k,i} \\ &= \sum_i x_{k,i} \ln x_{k,i} + \sum_i C_{k,i} x_{k,i} + \ln Z_k \sum_i x_{k,i} \end{aligned} \tag{35}$$

Since $\sum_i x_{k,i} = 1$, we obtain

$$\mathrm{KL}(x_k \| q_k) = \Big(\sum_i C_{k,i} x_{k,i} + \sum_i x_{k,i} \ln x_{k,i}\Big) + \ln Z_k \tag{36}$$

Thus,

$$\sum_i C_{k,i} x_{k,i} + \sum_i x_{k,i} \ln x_{k,i} \geq -\ln \sum_j e^{-C_{k,j}} \tag{37}$$

with equality iff $x_k = q_k$. Hence the following convex identity holds:

$$-\ln \sum_j e^{-C_{k,j}} = \min_{\substack{x_{k,i} \geq 0 \\ \sum_i x_{k,i} = 1}} \left\{ \sum_i C_{k,i} x_{k,i} + \sum_i x_{k,i} \ln x_{k,i} \right\} \tag{38}$$

To encode (38) with convex cones, introduce for all (k,i) auxiliary variables $f_{k,i}$ and enforce the relative-entropy epigraph

$$f_{k,i} \geq x_{k,i} \ln x_{k,i}, \qquad \forall k \in K,\ \forall i \in S \tag{39}$$

which can be modeled via the exponential cone as $(-f_{k,i},\, 1,\, x_{k,i}) \in \mathcal{K}_{\exp}$. Next, introduce $o_k \in \mathbb{R}$ and nonnegative $h_{k,i} \geq 0$ and impose the log-sum-exp epigraph

$$(-C_{k,i} - o_k,\, 1,\, h_{k,i}) \in \mathcal{K}_{\exp}, \quad \forall i \in S, \qquad \sum_{i \in S} h_{k,i} \leq 1 \tag{40}$$

which is equivalent to $o_k \geq \ln \sum_{i \in S} e^{-C_{k,i}}$.

Finally, enforce the following constraint together with the simplex conditions $x_{k,i} \geq 0$ and $\sum_i x_{k,i} = 1$:

$$\sum_{i \in S} \Big(C_{k,i}\, x_{k,i} + f_{k,i}\Big) + o_k = 0, \qquad \forall k \in K \tag{41}$$

By Gibbs inequality and (40), the equality is tight at optimality, which yields $x_{k,i} = q_{k,i}$.

3) Second-order cone power flow model

We convexify the AC power-flow model using a second-order cone programming relaxation.

Nodal power balance:

$$\sum_{k:\,(j,k)\in E} P_{jk} - \sum_{i:\,(i,j)\in E} \left(P_{ij} - R_{ij}\,\ell_{ij}\right) = P_j^d - P_j^g \quad (42)$$

$$\sum_{k:\,(j,k)\in E} Q_{jk} - \sum_{i:\,(i,j)\in E} \left(Q_{ij} - X_{ij}\,\ell_{ij}\right) = Q_j^d - Q_j^g \quad (43)$$

Voltage drop on branch:

$$v_j = v_i - 2\left(R_{ij}P_{ij} + X_{ij}Q_{ij}\right) + \left(R_{ij}^2 + X_{ij}^2\right)\ell_{ij}, \quad \forall (i,j) \in E \quad (44)$$

Second-order cone relaxation:

$$P_{ij}^2 + Q_{ij}^2 \;\le\; v_i\,\ell_{ij}, \quad \forall (i,j) \in E \quad (45)$$

Operational constraints:

$$\begin{aligned} &v_{\min} \le v_i \le v_{\max}, \quad 0 \le \ell_{ij} \le \bar{\ell}_{ij}, \\ &|P_{ij}| \le \bar{P}_{ij}, \quad |Q_{ij}| \le \bar{Q}_{ij}, \quad \forall (i,j) \in E \end{aligned} \quad (46)$$

4) Line overload

We define the loading rate ρ_i and overload severity τ_i as follows.

$$m_i = z_i / z_{i,rate}, \quad \forall i \in B \quad (47)$$

$$\tau_i \ge \rho_i - \Gamma, \quad \tau_i \ge 0, \quad \forall i \in B \quad (48)$$

In (13) we have $y_i^1 \in \{0,1\}$ indicate whether an overload occurs, using the Big-M method we obtain:

$$m_i - \Gamma \le M_l\, y_i^1, \quad \forall i \in B \quad (49)$$

$$m_i - \Gamma \ge \varepsilon_l\, y_i^1 - M_l\,(1 - y_i^1), \quad \forall i \in B \quad (50)$$

$$\tau_i \le M_l\, y_i^1, \quad \forall i \in B \quad (51)$$

5) Bus voltage violations

First, we define two non-negative variables π_i^+ and π_i^- and define $\mathcal{V}_i = v_i^2$, then we can get

$$\pi_i^- \;\ge\; \mathcal{V}_i - v_{\max}^2, \quad \forall i \in E \quad (52)$$

$$\pi_i^+ \;\ge\; v_{\min}^2 - \mathcal{V}_i, \quad \forall i \in E \quad (53)$$

Similar to the line overload part, we adopt the Big-M method and introduce binary indicators $\delta_i^+, \delta_i^- \in \{0,1\}$ to convert this part into convex form

$$\mathcal{V}_i \le V_{\max}^2 + M_v\,\delta_i^+, \quad \mathcal{V}_i \ge V_{\min}^2 - M_v\,\delta_i^-, \quad \forall i \in E \quad (54)$$

$$\pi_i^- \le M_v\,\delta_i^+, \quad \pi_i^+ \le M_v\,\delta_i^-, \quad \forall i \in E \quad (55)$$

$$\delta_i^+ + \delta_i^- \le 1, \quad \forall i \in E \quad (56)$$

6) Reconstruction of the EVCS Identification Model

Before reconstructing the target EVCS identification model, we reformulate constraint (13h) as:

$$0 \le n_i \le n_i^{\mathrm{ava}}\, s_i, \quad \forall i \in S \quad (57)$$

$$0 \le n_i \le a_i, \quad \forall i \in S \quad (58)$$

Thus, the original model can be reformulated as follows.

$$\min_{\Delta p, \Delta t, s} \; \psi \cdot \mathcal{C} \;-\; (1-\psi)\cdot J \quad (59a)$$

$$\text{s.t.} \quad C_{a,max} = \sum_{i\in\mathcal{S}} n_i^{ava}\left(c_i^p\,\overline{\Delta p}_i \;+\; c_i^t\,\overline{\Delta t}_i\right) \quad (59b)$$

$$\mathcal{C} = C_a / C_{a,max} \quad (59c)$$

$$C_{k,i} = (p_i^0 + \Delta p_i) + \omega\,(t_i^0 + \Delta t_i), \quad \forall k \in K,\ \forall i \in S \quad (59d)$$

$$\sum_{i\in S} x_{k,i} = 1, \quad x_{k,i} \ge 0, \quad \forall k \in K, \quad (59e)$$

$$n_j^{req} \;=\; \sum_{k\in\mathcal{K}} x_{kj}, \quad \forall j \in S \quad (59f)$$

$$\Delta z_{\mathrm{inj},e} = L \sum_{j\in S:\, b(j)=e} n_j\,\mathcal{A}_e, \quad \forall e \in E \quad (59g)$$

$$\sum_{i\in E}\left(\pi_i^+ + \pi_i^-\right) \ge \varepsilon_v \quad (59h)$$

$$\sum_{i\in B} \tau_i \ge \varepsilon_l \quad (59i)$$

$$s_i \in \{0,1\},\ \forall i \in S, \quad \bar{S} = \{\, i \in S \mid s_i = 1 \,\} \quad (59j)$$

$$\underline{\Delta p}_i \le \Delta p_i \le \overline{\Delta p}_i, \quad \forall i \in S \quad (59k)$$

$$\underline{\Delta t}_i \le \Delta t_i \le \overline{\Delta t}_i, \quad \forall i \in S \quad (59l)$$

$$c_i^p \ge 0, \quad c_i^t \ge 0, \quad \forall i \in S \quad (59m)$$

$$(25)-(32), (39)-(58) \quad (59n)$$

where M_l and M_v are Big-M constants; ε_l and ε_v are small positive constants.

The reconstructed model can be solved directly using a solver such as MOSEK.

B. Derivation of Parameter $\rho_t^{i,j}$

The attractiveness of an EVCS to drivers is influenced by time and charging price. Accordingly, the attractiveness index of EVCS i for EVCNS recommendations can be formulated as [38]:

$$U_t^i = -\lambda \cdot T_t^i - p_i(t) \cdot N_t, \forall i \in S \quad (60)$$

where U_t^i is the attractiveness index of EVCS i at time t; λ is the penalty coefficient that converts time into cost; T_t^i is the total time spent by EVs to reach EVCS i; $p_i(t)$ is the charging price of EVCS i at t.

When considering the competition between the target EVCS and another EVCS to equalize the attractiveness of the two EVCSs, it is given that

$$U_t^i - U_t^j = -\lambda \cdot (T_t^i - T_t^j) - N_t \cdot (p_i(t) - p_j(t)) = 0 \quad (61)$$

Therefore, we have:

$$\Delta p(t) = -\lambda (T_t^i - T_t^j)/N_t \quad (62)$$

Based on the charging price of EVCS j, the indifferent price can be shown as:

$$p_i^{**}(t) = p_j(t) + \Delta p(t) \tag{63}$$

It should be noted that $Pr = 0.5$ when EV drivers are indifferent between two EVCSs. Substituting (p_i^*, 0.5) into (20) we obtain:

$$f(\rho_t^{i,j}) = \rho_t^{i,j} e^{\rho_t^{i,j} p_i^{**}(t)} - 0.5 \tag{64}$$

This coefficient is obtained by the Newton Raphson method

$$\rho_{t,m+1}^{i,j} = \rho_{t,m}^{i,j} - \left[d(f(\rho_{t,m}^{i,j}))/d\rho_{t,m}^{i,j} \right]^{-1} \cdot f(\rho_{t,m}^{i,j}) \tag{65}$$

In addition, another critical requirement is to ensure that (64) has at least one root. Therefore, we need to let $f = 0$ to get the unique root.

$$0.5 = \rho_t^{i,j}\, e^{-\rho_t^{i,j} p_i^{**}(t)} \tag{66}$$

$$\ln(0.5) = \ln(\rho_t^{i,j}) - \rho_t^{i,j} p_i^{**}(t) \tag{67}$$

Define $\tau(\rho_t^{i,j})$ as

$$\tau(\rho_t^{i,j}) = \ln(\rho_t^{i,j}) - \rho_t^{i,j} p_i^{**}(t) - \ln(0.5) \tag{68}$$

Next, take the derivative of (68):

$$d\tau(\rho_t^{i,j})/d\rho_{\beta,t} = 1/\rho_t^{i,j} - p_i^*(t) = 0 \tag{69}$$

$$\rho_t^{i,j} = 1/p_i^{**}(t) \tag{70}$$

The global maximum point is $(1/p_i^{**}(t), e/p_i^{**}(t) - 0.5)$. Thus when $f(\rho_t^{i,j}) = 0$, $p_i^{**}(t) = 2/e$, this is the upper limit of price change. However, the true price change should satisfy $[p_{min}, p_{max}]$. A parameter $\lambda_i^*(t)$ is defined to shrink the real charging price into the range of $(0, 2/e]$.

$$\lambda_i^*(t) = (2/e)/p_{max} \cdot p_i(t) \tag{71}$$

C. Demand Probability for Multiple EVCS

The indifferent price of each pair of EVCS is first derived. The corresponding competitive demand probability is calculated based on the EVCS charging price using equation (20). For a CPTS with n EVCSs, there will be $n-1$ equations. The probability of competitive demand for each pair of EVCS satisfies (72).

$$Pr_i/Pr_j = \rho_t^{i,j} e^{\rho_t^{i,j} p_j(t)} / (1 - \rho_t^{i,j} e^{\rho_t^{i,j} p_j(t)}) \tag{72}$$

In addition, the sum of the probabilities of competitive demand for all EVCSs should be equal to 1. However, the probability of each pair of EVCSs is independently distributed. Therefore, the probability needs to be normalized. Denote the unnormalized probability of EVCS i as f_i.

$$f_i = \frac{1}{n-1} \sum_{j \in S, j \neq i} Pr_i = \frac{1}{n-1} \sum_{j \in S, j \neq i} \rho_t^{i,j} e^{-\rho_t^{i,j} \lambda_t^{*,i}} \tag{73}$$

Denote the normalization factor as $\mathcal{Z}$

$$\mathcal{Z} = \sum_{i \in S} f_j = \sum_{i \in S} \left(\frac{1}{n-1} \sum_{k \in S, k \neq i} f_k \right) \tag{74}$$

Algorithm 2 Dynamic Reference Vectors

Input: Archive A, adaptation interval ζ
if $t \bmod \zeta = 0$ **then**
  $\mathbf{f}_{\min} \leftarrow [\min(A.f_1), \min(A.f_2)]$
  $\mathbf{f}_{\max} \leftarrow [\max(A.f_1), \max(A.f_2)]$
  $\mathbf{V} \leftarrow \mathbf{V} \odot (\mathbf{f}_{\max} - \mathbf{f}_{\min})$
  for $j = 1$ to len($\mathbf{V}$) **do**
    if no_solution_near($\mathbf{V}[j], A$) **then**
      $\mathbf{V}[j] \leftarrow \upsilon \cdot \mathbf{V}[j]$
    end if
  end for
end if

Algorithm 3 Particle Update

Input: Particle $\mathbf{x}_i$, archive A, L_0-norm threshold ξ
conv_rank $\leftarrow$ non_dominated_rank($\mathbf{x}_i, A$)/$|A|$
$w_i \leftarrow w_{\min} + (w_{\max} - w_{\min}) \cdot (1 - \text{conv\_rank}^2)$
if f_2 is L_0-norm and $L_0(\mathbf{x}_i) > \gamma$ **then**
  $\mathbf{x}_i \leftarrow$ zero_mask($\mathbf{x}_i, p$)
else
  $\mathbf{x}_i \leftarrow \mathbf{x}_i + \mathcal{N}(0, \sigma = 1/t)$
end if
return $w_i, \mathbf{x}_i$

Algorithm 4 Archive Manager

Input: Candidate solutions C, reference vectors $\mathbf{V}$, angle threshold $\theta = \pi/\iota$
$C \leftarrow$ filter_epsilon_dominated(C, ϵ-grid)
$A_{\text{new}} \leftarrow \emptyset$
for $\mathbf{v} \in \mathbf{V}$ **do**
  sector $\leftarrow \{\mathbf{x} \in C \mid \text{angle}(\mathbf{x}, \mathbf{v}) < \theta\}$
  if sector $\neq \emptyset$ **then**
    $A_{\text{new}} \leftarrow A_{\text{new}} \cup \{\text{non\_dominated\_sort(sector)}[0]\}$
  end if
end for
return A_{new}

The normalized probability of EVCS i is

$$\Pr_{N_t^i} = \frac{f_i}{\mathcal{Z}} = \frac{\frac{1}{n-1} \sum_{j \in S, j \neq i} \rho_t^{i,j} e^{-\rho_t^{i,j} \lambda_t^{*,i}}}{\sum_{i \in S} \left(\frac{1}{n-1} \sum_{k \in S, k \neq i} \rho_t^{i,k} e^{-\rho_t^{i,k} \lambda_i^*(t)} \right)} \tag{75}$$

The sum of the probability of competitive demand for all EVCSs should be 1, i.e.

$$P_{r_{N_t^i}} + \sum_{j \in S, j \neq i} P_{r_{N_t^j}} = 1 \tag{76}$$

D. The Sub-Algorithms of Algorithm 1

E. Range of Values for Parameter k

When deriving k we consider the extreme case: if $\frac{N_i(t)}{N_{total}(t)} = 0$: $\kappa(t) = k \cdot (1 - \alpha)$, if $\frac{N_i(t)}{N_{total}(t)} = 1$: $\kappa(t) = k \cdot (\alpha \cdot 1 + (1 - \alpha)) = k$. Therefore, $\kappa(t) \in [k \cdot (1 - \alpha), k]$. Based on constraints in (24) we can get

$$\delta(t) \geq p_i^*(t) - \min_{j \neq i} p_j^*(t) + \epsilon_p \tag{77}$$

Let $\Delta p(t) = p_i^*(t) - \min_{j\neq i} p_j^*(t)$.

$$\kappa(t) \geq (\Delta p(t) + \epsilon_p)/(\Delta p(t) + \epsilon) \tag{78}$$

In the most stringent case $\Delta p(t) = 0$, we have $\kappa(t) \geq \frac{\epsilon_p}{\epsilon}$.

$$k \geq \frac{\epsilon_p}{\epsilon \cdot (1-\alpha)} \tag{79}$$

Based on the stealth constraint we can get

$$\kappa(t) \leq \frac{p_i^*(t) - (\mu_p - \gamma\sigma_p)}{p_i^*(t) - \min_{j\neq i} p_j^*(t) + \epsilon} \tag{80}$$

In the most stringent case, $p_i^*(t) \approx \mu_p$, $\min_{j\neq i} p_j^*(t) \approx \mu_p$. we obtain $\kappa(t) \leq \frac{\gamma\sigma_p}{\epsilon}$, and substituting $\kappa(t)$:

$$k \leq \frac{\gamma\sigma_p}{\epsilon} \tag{81}$$

The attack magnitude is converted to

$$\delta(t) = (\Delta p(t) + \epsilon) \cdot \kappa(t) \tag{82}$$

The goal is to ensure $\delta(t) \in [\delta_{min}, \delta_{max}]$. Substituting $\kappa(t)$:

$$\frac{\delta_{min}}{\Delta p(t) + \epsilon} \leq \kappa(t) \leq \frac{\delta_{max}}{\Delta p(t) + \epsilon} \tag{83}$$

In the most stringent case, $\Delta p(t) \approx 0$:

$$\frac{\delta_{min}}{\epsilon} \leq \kappa(t) \leq \frac{\delta_{max}}{\epsilon} \tag{84}$$

Substituting $\kappa(t)$ and combine all constraints, we can have:

$$k \in \left[\max\left(\frac{\epsilon_p}{\epsilon(1-\alpha)}, \frac{\delta_{min}}{\epsilon(1-\alpha)}\right), \min\left(\frac{\gamma\sigma_p}{\epsilon}, \frac{\delta_{max}}{\epsilon}\right)\right] \tag{85}$$

REFERENCES

[1] R. Ma and S. Bu, "Evaluation and mitigation of carbon emissions in energy industry," *Renew. Sustain. Energy Rev.*, vol. 212, p. 115329, 2025.

[2] S. Zhang, W. Chen, Q. Zhang, V. Krey, E. Byers, P. Rafaj, B. Nguyen, M. Awais, and K. Riahi, "Targeting net-zero emissions while advancing other sustainable development goals in china," *Nature Sustain.*, vol. 7, no. 9, pp. 1107–1119, 2024.

[3] Z. Yang, Y. Xiang, K. Liao, and J. Yang, "Research on security defense of coupled transportation and cyber-physical power system based on the static bayesian game," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 3, pp. 3571–3583, 2022.

[4] L. Xu, C. Dou, D. Yue, H. Li, and Y. Ji, "Cyber-physical-transportation system based co-design of charging pricing and frequency regulation control for evs in multi-market," *Protection Control Modern Power Syst.*, vol. 10, no. 6, pp. 1–14, 2025.

[5] S. Powell, G. V. Cezar, L. Min, I. M. Azevedo, and R. Rajagopal, "Charging infrastructure access and operation to reduce the grid impacts of deep electric vehicle adoption," *Nat. Energy*, vol. 7, no. 10, pp. 932–945, 2022.

[6] W. Liu, X. Shi, J. Zhao, X.-P. Zhang, and Y. Xue, "Electric vehicle charging simulation framework considering traffic, user, and power grid," *J. Modern Power Syst. Clean Energy*, vol. 9, no. 3, pp. 602–611, 2021.

[7] S. Bu, L. G. Meegahapola, D. P. Wadduwage, and A. M. Foley, "Stability and dynamics of active distribution networks (adns) with d-pmu technology: A review," *IEEE Trans. Power Syst.*, vol. 38, no. 3, pp. 2791–2804, 2023.

[8] Z. Wang and S. Bu, "Design and defense of modal resonance-oriented cyber-attack against wide-area damping control," *IEEE Trans. Smart Grid*, 2023.

[9] Y. Wang, J. Li, J. Qiu, and Y. Chen, "Adaptive early warning method of cascading failures caused by coordinated cyber-attacks," *CSEE J. Power and Energy Syst.*, vol. 11, no. 1, pp. 406–423, 2025.

[10] A. Abazari, M. M. Soleymani, S. Marandi, M. Ghafouri, C. Assi, D. Jafarigiv, and R. Atallah, "Electric vehicle-based load-altering attacks and their impacts on power grids operations," *IEEE Rel. Mag.*, 2024.

[11] A. Abazari, K. Sarieddine, M. Ghafouri, D. Jafarigiv, R. Atallah, and C. Assi, "Electric vehicle switching attacks against subsynchronous stability of power systems," *IEEE Trans. Ind. Informat.*, 2024.

[12] M. E. Kabir, M. Ghafouri, B. Moussa, and C. Assi, "A two-stage protection method for detection and mitigation of coordinated evse switching attacks," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4377–4388, 2021.

[13] F. Wei and X. Lin, "Cyber-physical attack launched from evse botnet," *IEEE Trans. Power Syst.*, vol. 39, no. 2, pp. 3603–3614, 2023.

[14] H. An, J. Yi, G. Zhang, O. Bamisile, J. Li, Q. Huang *et al.*, "A robust v2g voltage control scheme for distribution networks against cyber attacks and customer interruptions," *IEEE Trans. Smart Grid*, 2024.

[15] A. Abazari, M. M. Soleymani, M. Ghafouri, D. Jafarigiv, R. Atallah, and C. Assi, "Deep learning detection and robust mpc mitigation for ev-based load-altering attacks on wind-integrated power grids," *IEEE Trans. Ind. Cyber-Phys. Syst.*, 2024.

[16] S. Acharya, Y. Dvorkin, and R. Karri, "Public plug-in electric vehicles+ grid data: Is a new cyberattack vector viable?" *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5099–5113, 2020.

[17] M. A. Sayed, M. Ghafouri, R. Atallah, M. Debbabi, and C. Assi, "Grid chaos: An uncertainty-conscious robust dynamic ev load-altering attack strategy on power grid stability," *Appl. Energy*, vol. 363, p. 122972, 2024.

[18] M. M. Soleymani, A. Abazari, M. Ghafouri, D. Jafarigiv, R. Atallah, and C. Assi, "Data-enabled modeling and pmu-based real-time localization of ev-based load-altering attacks," *IEEE Trans. on Smart Grid*, vol. 15, no. 6, pp. 6063–6079, 2024.

[19] J. Jin and Y. Xu, "Shortest-path-based deep reinforcement learning for ev charging routing under stochastic traffic condition and electricity prices," *IEEE Internet Things J.*, vol. 9, no. 22, pp. 22 571–22 581, 2022.

[20] S. Shirvani, Y. Baseri, and A. Ghorbani, "Evaluation framework for electric vehicle security risk assessment," *IEEE Trans. Intell. Transp. Syst.*, 2023.

[21] K. Li, C. Shao, M. Shahidehpour, and X. Wang, "A capacity-based regulation method for coordinating electric vehicle charging flows in coupled distribution and transportation networks," *IEEE Trans. Smart Grid*, vol. 15, no. 3, pp. 3066–3079, 2023.

[22] Y. Li, S. Su, M. Zhang, Q. Liu, X. Nie, M. Xia, and D. D. Micu, "Multi-agent graph reinforcement learning method for electric vehicle on-route charging guidance in coupled transportation electrification," *IEEE Trans. Sustain. Energy*, vol. 15, no. 2, pp. 1180–1193, 2023.

[23] O. G. M. Khan, F. Elghitani, A. Youssef, M. Salama, and E. El-Saadany, "Real-time congestion-aware charging station assignment model for evs," *IEEE Internet Things J.*, 2023.

[24] L. Ran, J. Qin, Y. Wan, W. Fu, W. Yu, and F. Xiao, "Fast charging navigation strategy of evs in power-transportation networks: A coupled network weighted pricing perspective," *IEEE Trans. Smart Grid*, vol. 15, no. 4, pp. 3864–3875, 2024.

[25] A. R. Bagabaldo, Q. Gan, A. M. Bayen, and M. C. González, "Impact of navigation apps on congestion and spread dynamics on a transportation network," *Data Sci. Transp.*, vol. 6, no. 2, p. 12, 2024.

[26] Y. Feng, S. E. Huang, W. Wong, Q. A. Chen, Z. M. Mao, and H. X. Liu, "On the cybersecurity of traffic signal control system with connected vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 16 267–16 279, 2022.

[27] S. Guo, Y. Lin, S. Li, Z. Chen, and H. Wan, "Deep spatial–temporal 3d convolutional neural networks for traffic data forecasting," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 10, pp. 3913–3926, 2019.

[28] K.-D. Lu, Z.-G. Wu, and T. Huang, "Differential evolution-based three stage dynamic cyber-attack of cyber-physical power systems," *IEEE/ASME Trans. Mechatronics*, vol. 28, no. 2, pp. 1137–1148, 2023.

[29] M. Elassy, M. Al-Hattab, M. Takruri, and S. Badawi, "Intelligent transportation systems for sustainable smart cities," *Transportation Engineering*, vol. 16, p. 100252, 2024.

[30] Z. Garofalaki, D. Kosmanos, S. Moschoyiannis, D. Kallergis, and C. Douligeris, "Electric vehicle charging: A survey on the security issues and challenges of the open charge point protocol (ocpp)," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 3, pp. 1504–1533, 2022.

[31] A. Akbarian, M. Bahrami, M. Ahmadi, M. Vakilian, and M. Lehtonen, "Detection of cyber attacks to mitigate their impacts on the manipulated ev charging prices," *IEEE Trans. Transport. Electrific*, vol. 10, no. 4, pp. 8881–8892, 2024.

[32] T. Zhang, W. Zhang, Q. Zhao, Z. Li, and J. Zhao, "Forecasting-aided joint topology/state estimation for distribution systems via bayesian non-parametric modeling," *IEEE Trans. Smart Grid*, vol. 15, no. 1, pp. 1014–1029, 2024.

[33] S. Radhoush, T. Vannoy, B. M. Whitaker, and H. Nehrir, "Random forest meta learner for generating pseudo-measurements in active distribution power networks," in *Proc. IEEE Power Energy Soc Innov Smart Grid Technol Conf.*, 2023, pp. 1–5.

[34] A. Khaleghi, M. S. Ghazizadeh, and M. R. Aghamohammadi, "A deep learning-based attack detection mechanism against potential cascading failure induced by load redistribution attacks," *IEEE Trans. Smart Grid*, vol. 14, no. 6, pp. 4772–4783, 2023.

[35] K. Li, C. Shao, M. Shahidehpour, and X. Wang, "A capacity-based regulation method for coordinating electric vehicle charging flows in coupled distribution and transportation networks," *IEEE Trans. Smart Grid*, vol. 15, no. 3, pp. 3066–3079, 2023.

[36] X. Shi, Y. Xu, Q. Guo, H. Sun, and W. Gu, "A distributed ev navigation strategy considering the interaction between power system and traffic network," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 3545–3557, 2020.

[37] Q. Xing, Y. Xu, Z. Chen, Z. Zhang, and Z. Shi, "A graph reinforcement learning-based decision-making platform for real-time charging navigation of urban electric vehicles," *IEEE Trans. Ind. Informat.*, vol. 19, no. 3, pp. 3284–3295, 2022.

[38] S. Lai, J. Qiu, Y. Tao, and J. Zhao, "Pricing for electric vehicle charging stations based on the responsiveness of demand," *IEEE Trans. Smart Grid*, vol. 14, no. 1, pp. 530–544, 2022.

[39] Y. Sheng, Q. Guo, T. Yang, Z. Zhou, and H. Sun, "A potential security threat and its solution in coupled urban power-traffic networks with high penetration of electric vehicles," *CSEE J. Power Energy Syst.*, vol. 8, no. 4, pp. 1097–1109, 2022.

[40] R. Ma and S. Bu, "Supplementary material for 'design of joint cyber-attacks on electric vehicle charging via pricing and traffic manipulation to threaten secure operation of power system'," 2025, [online] Available: https://github.com/RZ-Ma/PES2025.

[41] D. Gotti, H. Amaris, and P. L. Larrea, "A deep neural network approach for online topology identification in state estimation," *IEEE Trans. Power Syst.*, vol. 36, no. 6, pp. 5824–5833, 2021.