Load Redistribution Attack for Power Systems with High Penetration of EVs

Zelin Liu *†, Tao Liu *†, Yue Song *‡, and David J.Hill §
* Department of Electrical and Electronic Engineering
The University of Hong Kong, Hong Kong S.A.R, China
† Shenzhen Institute of Research and Innovation,
The University of Hong Kong, Shenzhen, China
‡ Department of Control Science and Engineering
Tongji University, Shanghai, China
§Department of Electrical and Computer System Engineering,
Monash University, Melbourne, Australia

***Abstract*—This paper provides insights for cyber defenders of power systems with high penetration of electric vehicles (EVs) by proposing a novel consecutive attack model based on load redistribution for price control in both transmission networks (TNs) and distribution networks (DNs). The target of the attack is to induce massive EV users in DNs to charge simultaneously and cause a spike of loads in the TN at peak hours. The problem is formulated as a multi-slot bi-level optimization problem, where the upper level describes the hacker behavior and attacking constraints. The lower level explains the TN operator and DN operators' behaviors and the relationship between the local marginal price and retail charging price. The bi-level problem is converted into an equivalent single-level mix-integer linear problem and is solved based on greedy algorithm. Simulations on IEEE 30-bus system prove the effectiveness of the attack strategy.**

***Index Terms*—False data injection attack, load redistribution attack, electric vehicle, bi-level optimization**

I. Introduction

Driven by the increasing environmental pressure, governments are promoting the development of electric vehicles (EVs) all over the world. Due to the high individual uncertainty of EV charging behavior, new planning and control strategies should be considered especially for high EV penetration networks. Generally, power system operators wish to reduce the number of charging EVs in residential loads during daily peak hours to reduce the risk of branch overflow and system costs. Since individual charging behaviors of EVs are strongly correlated with the local electric price at the EV station, price control is a general method that is widely adopted by the operators. When the system residential load is at its peak hour, the transmission network operators (TNOs) increase the local marginal prices (LMPs) on congested buses to avoid branch overflow. The distribution network operators (DNOs) on these congested buses monitor the wholesale price change, and increase the charging price of EV stations accordingly to maximize their benefits. Thus, the EV charging behaviors are discouraged by the high charging price [1]. Figure 1 illustrates the price scheme in a high EV penetrated network.

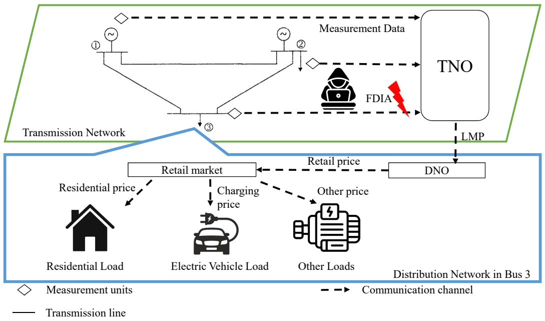


Fig. 1: Price scheme in high EV penetrated network

Since LMPs in transmission networks are strongly correlated with branch congestion, if attackers hijack the communication channels and corrupt the measurement data, then TNOs will have a wrong judgment on the system state and set false LMPs [2]. Therefore, a stealthy false data injection attack (FDIA) may disable the whole price control scheme and trigger a load surge during peak hours [3]. Such a load surge may cause branch overflow, load shedding, voltage reduction or frequency instability [4]. Thus, the analysis and modeling of FDIA in price control of high EV penetration networks is critical for the secure operation of power systems.

High EV penetration networks can be vulnerable to cyber-physical threats since the hacker may launch the attack at any time at any place [5]. The high power demand in EV loads may destabilize the system under small attacks [6]. FDIA can disrupt the data market forecasts and impose operating threats to EV charging stations [7]. Moreover, algorithms for EV load tracking and management enable the hacker to predict daily EV demand based on historical communication data. Jaruwatanachai *et al.* suggests that there is a strong correlation between time-of-use price and EV charging demand [8]. A conditional random field method is proposed by Soltani *et al.*

Submitted to the 23rd Power Systems Computation Conference (PSCC 2024). The work was supported by the National Natural Science Foundation of China through Project No.62173287 and the Research Grants Council of the Hong Kong Special Administrative Region under the General Research Fund through Project No.17209219. *(Corresponding author: Tao Liu.)*

to track the real-time load elasicity based on previous data [9]. Such preditions may result in privacy exposure of EV users. FDIAs on high EV penetrated networks pose a serious threat to the whole national industry. Frequency can sharply increase or decrease in response to sudden drops or spikes in EV loads, which may cause the generation output oscillations and reduce the lifetime of the generators [6]. Simultaneous fast charging of EVs can also cause system voltage issues, which may result in voltage limit violation, distribution system asset over-loading, or even blackouts [10].

Based on diverse attacking resources, attacks on electric price can be various [11]. To manipulate the electric market, the hackers can directly jam the price control signal from the control center and cease the jamming when the price is significantly changed [12]. In order to bypass the BDD test, hackers make use of measurement units on loads and branches to transmit fake data to the control center [13]. Different attacking objectives decide the damage that can be caused by the attack. Xie *et al.* focus on creating profitable financial misconduct such as virtual bidding at certain buses [14]. Jia *et al.* proposes a method to maximize profits for certain generator buses [13]. Furthermore, with a specially designed attacking vector, hackers are able to launch the attack under limited measurement data [15] and manipulate LMPs on tagged buses [16]. However, the state-of-the-art methods only focus on LMPs in transmission networks, which is not applicable to EV charging prices in distribution networks.

Instead of directly manipulating the price control signal or the EV station communication infrastructure, we propose a novel attack method that can mislead the DNOs to set the wrong electrical prices for EV stations and therefore cause EVs to charge at the same time during peak hours. The method is based on a special type of FDIA, load redistribution attack (LRA) model, and it only manipulates the residential load bus signals in the transmission network. Rather than focusing on increase the system cost like traditional LRA method, our algorithm aims to affect the LMP on certain EV buses. A lower level optimization problem representing the correlation between LMP and charging price is attached to the original model. Both instant attacks and consecutive attacks are considered to address the potential damage they may cause to the system.

The rest of the paper is organized as follows. Section II gives a brief review of the LRA model and formulates the attack problem. Section III introduces the attack model. The effectiveness of the proposed method is tested on the IEEE 30-bus system in Section IV. Section V concludes the paper.

II. Problem Formulation

Since EV stations are generally located in a distribution network and the FDIA is launched in the transmission network, we will introduce the electric price scheme in a connected transmission and distribution network. In this paper, we assume that there is only one aggregated distribution network under a transmission EV bus. We will explain the procedure of LRA and its affect on LMP in the transmission network.

A. Electrical Price Scheme in Transmission Network

We consider a power system with N_l transmission lines and N buses, including N_g generator buses, N_d residential load buses, and N_{EV} EV buses. Here, an EV bus is a load bus in transmission network that its aggregated distribution network has 100% EV loads. We use the notations $\mathcal{L}$, $\mathcal{N}$, $\mathcal{G}$, $\mathcal{D}$ and $\mathcal{V}$ to represent the index sets of transmission lines, buses, generator buses, residential load buses and EV load buses. The bus index is arranged with generator buses at the beginning, followed by residential load buses, and EV load buses afterward. For a connecting bus that has no generator or load, we treat it as a load bus with its load equal to zero.

In a real-time electricity market, TNOs minimize the system cost by predicting the load and solving the following optimal power flow (OPF) problem to determine the LMPs

$$\min_{P^t_{G_i}} \sum_{i=1}^{N_g} c_i^t P^t_{G_i} \quad \forall i \in \mathcal{G} \tag{1a}$$

$$s.t. \quad \sum_{i=1}^{N_g} P^t_{G_i} = \sum_{j=1}^{N_d} P^t_{L_j} + \sum_{k=1}^{N_{EV}} P^t_{EV_k} \tag{1b}$$

$$\sum_{k\in\mathcal{N}} T_{i,k} P^t_k = P^t_{line,i} \quad \forall i \in \mathcal{L} \tag{1c}$$

$$-P^{max}_{line,i} \leq P^t_{line,i} \leq P^{max}_{line,i} \quad \forall i \in \mathcal{L} \tag{1d}$$

$$P^{min}_{G_i} \leq P^t_{G_i} \leq P^{max}_{G_i} \quad \forall i \in \mathcal{G}, \tag{1e}$$

where $P^t_{G_i}$, $P^t_{L_i}$, $P^t_{EV_i}$ are generation outputs, residential loads, and EV loads on bus i, $\forall i \in \mathcal{N}$ at time t. P^t_i is the net power output on bus i, $\forall i \in \mathcal{N}$ at time t. c^t_i is the unit power cost on generator bus i, $\forall i \in \mathcal{G}$ at time t. $T_{i,k}$ is the power transfer distribution factor (PTDF) of branch i, $\forall i \in \mathcal{L}$ to bus k, $\forall k \in \mathcal{N}$. $P^{max}_{line,i}$ is the branch flow limit on transmission line i, $\forall i \in \mathcal{L}$. $P^{min}_{G_i}$ and $P^{max}_{G_i}$ are minimum and maximum generation output on bus i, $\forall i \in \mathcal{G}$. Objective (1a) indicates that the TNO plan to minimize the system cost during operation. Constraint (1c) and (1d) calculates the branch power flow and bounds it by branch capacity. Constraint (1b) is the power balance equation and (1e) is the generation constraint.

The LMP at bus k, $\forall k \in \mathcal{N}$ can be calculated through the following equation [13]:

$$\lambda^t_k = \widetilde{\lambda}^t - \sum_j T_{j,k}(\pi^+_{j,t} - \pi^-_{j,t}), \tag{2}$$

where λ^t_k is the LMP at bus k, $\forall i \in \mathcal{N}$ at time t. $\widetilde{\lambda}^t$, $\pi^+_{j,t}$ and $\pi^-_{j,t}$, $\forall j \in \mathcal{L}$ are dual variables corresponding to the power balance equation (1c) and line flow constraints (1d). $\widetilde{\lambda}^t$ is the least incremental cost in the system and is globally identical for all the system buses. The term $\sum_j T_{j,k}(\pi^+_{j,t} - \pi^-_{j,t})$ in (2) defines the congestion cost of bus k at time t.

Generally, TNOs will predict the load level before the dispatch interval and solve (1) to determine an ex-ante LMP for each bus. Since the predicted load level might be different from the real situation, the TNOs will observe the real network congestion situation from the measurement units to determine the dual variables $\pi^+_{j,t}$, $\pi^-_{j,t}$ and calculate the ex-post LMPs through (2) after the dispatch interval. From complementary slackness in the Karush-Kuhn-Tucker (KKT) condition, it is clear that when a branch j, $\forall j \in \mathcal{L}$ reaches its maximum limit at time t, $\pi^{+}_{j,t}$ and $-\pi^{-}_{j,t}$, $\forall j \in \mathcal{L}$ will change from zero to a positive value and thus raise the congestion cost and ex-post LMPs as shown in (2) [17]. In this paper, we assume that some branches around certain EV buses will reach its maximum limit during peak hours and consequently induce a congestion cost increase on these EV buses.

B. Load Redistribution Attack in Transmission Network

As a practical type of FDIA, LRAs only manipulate measurement units on load buses and branches [18]. Connecting buses and buses with generators are assumed to be well-protected and cannot be attacked. Therefore, the total load of the system should remain unchanged during the attack to avoid the violation of Kirchhoff's Current Law. In an LRA, the hacker fakes the measurement data to disturb the system state estimation and misleads the operator to design a worse generation strategy. We use the following bi-level optimization model to illustrate the traditional LRA method:

$$\max_{\Delta P^t_{L_i}} \quad \sum_{i=1}^{N_g} c_i^t P_{Gi}^{*,t} \tag{3a}$$

$$s.t. \quad \sum_{i=1}^{N_d} \Delta P^t_{L_i} = 0 \quad \forall i \in \mathcal{D} \tag{3b}$$

$$\sum_{k \in \mathcal{N}} T_{i,k} \Delta P^t_k = \Delta P^t_{line,i} \quad \forall i \in \mathcal{L} \tag{3c}$$

$$-\tau P^{t-1}_{L_i} \le \Delta P^t_{L_i} \le \tau P^{t-1}_{L_i} \quad \forall i \in \mathcal{D} \tag{3d}$$

$$\sum_{i=1}^{N_d} \delta^t_{L,i} + \sum_{j=1}^{N_l} \delta^t_{line,j} \le R \tag{3e}$$

$$P^{*,t}_{G_i} = \arg\min_{P_{G_i}} \{\sum_{i=1}^{N_g} c_i^t P^t_{G_i}\} \quad \forall i \in \mathcal{G} \tag{3f}$$

$$(1b) - (1e),$$

where $\Delta P^t_{L_i}$, $\Delta P^t_{line,j}$ is the false data injection change on residential load i, $\forall i \in \mathcal{D}$ and branch j, $\forall j \in \mathcal{L}$ at time t. ΔP^t_i is the net power output change on bus i, $\forall i \in \mathcal{N}$ at time t. $\delta^t_{L,i}$ and $\delta^t_{line,j}$ are binary variables that reflect if the measurement units on residential load i, $\forall i \in \mathcal{D}$ or branch j, $\forall j \in \mathcal{N}$ are changed after the attack at time t. R is the attack resources limitation and τ is the attack magnitude limit. argmin$\{\bullet\}$ represents the arguments of the minima. The upper level problem, including (3a)-(3e), stands on the hacker's perspective, which wishes to maximize the total system cost after the attack. Constraint (3b) ensures that the total load of the system is unchanged during the attack. Constraints (3c) and (3d) are attacking magnitude limit and attacking resources limit, respectively. The lower level problem consists of (3f), (1b)-(1e) and is an OPF problem that represents the TNO's perspective during the attack. $P^{*,t}_{G_i}$ is the optimal generation strategy after the TNO solves the OPF problem (3f), (1b)-(1e).

Although the LMP is not included in the LRA model (3), hackers manipulate the branch power flow data during the attack as shown in constraint (3c). This indicates that the TNO recieves wrong branch flow data and consequently make wrong judgments of branch power flow during the LRA. Recall that in (2), the congestion cost of the LMP is related to the dual variables of branch flow limits (1d). The wrong judgment of branch flow after an LRA might cause different dual variables in calculating the congestion cost of LMP, which leads to an electrical price change in EV stations.

C. Electrical Price Scheme in Distribution Network

Consider a distribution network with 100% EV loads, DNOs are supposed to buy electricity from the wholesale market and sell it to users based on retail market price [19]. Unlike the price scheme in transmission networks, the charging price in a retail market is not only related to the load level, but also depends on historical prices. EV users will compare the charging price on different time to decide their charging behaviors. Since we are considering a distribution network with a large number of EVs, the computational complexity for modeling every EV is extremely high. Thus, we use an aggregated EV model [19] to avoid introducing large number of variables. Assume that the DNO in this network wish to maximize their profit, the following optimization problem is applied as an electrical price scheme for the network:

$$\max_{\mu_k^t} \quad (\mu_k^t - \lambda_k^t) P^t_{EV_k} - O(P^t_{EV_k}) \quad \forall k \in \mathcal{V} \tag{4a}$$

$$s.t. \quad P^t_{EV_k} = P^{t,0}_{EV_k}(1 + \sum_{i=1}^{t} E^{t,i}(\mu_k^i / \mu_k^{i,0} - 1)) \quad \forall k \in \mathcal{V} \tag{4b}$$

$$0 \le P^t_{EV_k} \le P_{EV_{max}} \quad \forall k \in \mathcal{V}, \tag{4c}$$

where μ_k^t, λ_k^t are the average charging price in the retail market and the wholesale market price on EV bus k, $\forall k \in \mathcal{V}$ at time t, respectively. Noted that in this paper, we just use the ex-post LMP λ_k^t at bus k, $\forall k \in \mathcal{V}$ as the wholesale market price for DNOs. $P^t_{EV_k}$ is the total EV load in EV bus k, $\forall k \in \mathcal{V}$ at time t. $O(P^t_{EV_k}) = b_0 P^{t^2}_{EV_k} + b_1 P^t_{EV_k} + b_2$ is the management and operating cost function of the DNO. By using retail market income minus the wholesale market cost and operating cost, objective (4a) reflects the profits of the DNO. Constraint (4b) explains the relationship between charging price and charging behavior. Here, we use the elasticity coefficient $E^{t,i}$ to reflect the temporal elasticity correlation between the charging price at time t and time i [20]. With a basic EV charging demand $P^{t,0}_{EV_k}$ and basic EV charging price $\mu_k^{t,0}$, EV users adjust their charging behavior based on the change of charging price. Constraint (4c) ensures that the total EV load at bus k, $\forall k \in \mathcal{V}$ is within its maximum limit.

After modeling the LRA, the electrical price scheme in the transmission network and distribution network, we still have the following three problems that need to be solved.

- Although an LRA can mask the congestion scenario in branch power flow, how to introduce LMP into the LRA?
- To mislead charging behaviors of EV users, how to introduce the charging price into the LRA model?
- Since the electric price in a distribution network has temporal correlation with the historical data, how to

combine the price scheme in distribution network (4) with LRA model (3) and solve them?

We will answer these questions in the next section by proposing our attack model.

III. Proposed Model

Before introducing our attack model, two assumptions should be introduced. Since there are many FDIA methods such as blind attack [21], regional attack [22] for attacks without network parameters and the focus of this paper is to explore the LRA in system with high EV penetration, we assume that hackers have full knowledge of transmission network parameters. Moreover, hackers also have the EV load elasticity coefficient matrix $E^{t,i}$, basic charging demand $P^{t,0}_{EV_k}$ and basic charging price $\mu_k^{t,0}$ from historical EV data [20].

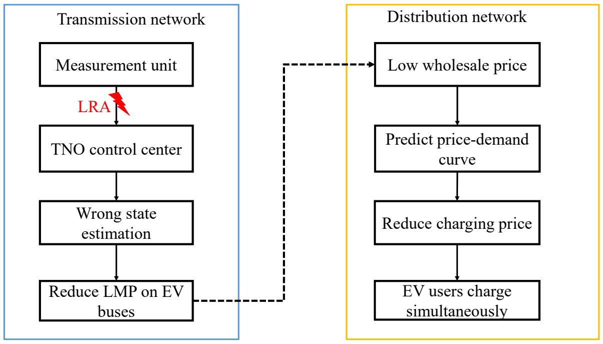


Fig. 2: Attack procedure

The goal of our model is to mislead the EV users to charge simultaneously at peak hours under the logical assumption that the TNO will minimize system costs and DNOs wish to maximize their own benefits. The attack procedure is shown in Fig. 2. During peak hours, the hacker launches an LRA on measurement units in the transmission network and misleads the TNO to get a wrong state estimation. Based on this wrong state estimation, TNO will design a new generation strategy and reduce the LMP on all EV buses. The DNOs in these EV buses monitor the wholesale price change and predict the price-demand curve to design new charge price. In order to maximize their benefits like (4), DNOs decrease the charging price in the retail market. The EV users observe the charging price reduction and start to charge their EVs at the same time resulting in a spike of loads. We use a multi-slot, bi-level optimization model to illustrate our new attack method:

$$\max_{\Delta P^t_{L_i}} \sum_{t=t_0}^{t_m} \sum_{i=1}^{N_{EV}} P^t_{EV_i} \quad \forall i \in \mathcal{V} \tag{5a}$$

$$s.t. \quad (3b)-(3e),(1b),(1d)-(1e)$$

$$\sum_{i=1}^{N_g} P^t_{Gi} = \sum_{j=1}^{N_d} P^t_{L,j} + \sum_{k=1}^{N_{EV}} P^{t-1}_{EV,k} \tag{5b}$$

$$\sigma^+_{i,t}, \sigma^-_{i,t}, \pi^+_{j,t}, \pi^-_{j,t} > 0 \quad \forall i \in \mathcal{G} \quad \forall j \in \mathcal{L} \tag{5c}$$

$$\sigma^+_{i,t}(P_{G_i} - P^{max}_{G_i}) = 0 \quad \forall i \in \mathcal{G}, \tag{5d}$$

$$\sigma^-_{i,t}(P_{G_i} - P^{min}_{G_i}) = 0 \quad \forall i \in \mathcal{G} \tag{5e}$$

$$\pi^+_{j,t}(\sum_{k\in\mathcal{N}} T_{j,k}P^t_k - P^{max}_{line,j}) = 0 \quad \forall j \in \mathcal{L} \tag{5f}$$

$$\pi^-_{j,t}(\sum_{k\in\mathcal{N}} T_{j,k}P^t_k + P^{max}_{line,j}) = 0 \quad \forall j \in \mathcal{L} \tag{5g}$$

$$c^t_i - \widetilde{\lambda}^t + \sigma^+_{i,t} - \sigma^-_{i,t} + T^T_{:,i}\pi^+_{:,t} - T^T_{:,i}\pi^-_{:,t} = 0 \quad \forall i \in \mathcal{G} \tag{5h}$$

$$\lambda^t_k = \widetilde{\lambda}^t - \sum_{i,j\in\mathcal{L}} T_{ij,k}(\pi^+_{ij,t} - \pi^-_{ij,t}) \quad \forall k \in \mathcal{V} \tag{5i}$$

$$\mu^t_k = \arg\max_{\mu^t_k}\{(\mu^t_k - \lambda^t_k)P^t_{EV_k} - O(P^t_{EV_k})\} \quad \forall k \in \mathcal{V} \tag{5j}$$

$$s.t. \quad (4b)-(4c). \tag{5k}$$

In (5h), $T_{:,i}$ is the $i-th$ column of matrix T. $\pi^+_{:,t} = (\pi^+_{1,t}, \pi^+_{2,t}, \pi^+_{3,t}, ...\pi^+_{N_l,t})$ is a column variable consists of dual variables $\pi^+_{j,t}$ with $j \in \mathcal{L}$. $(\bullet)^T$ refers to the transpose of a matrix or vector. Model (5) consists of two levels. (5a)-(5i) are the upper-level problem that illustrates the attack in the transmission network and (5j)-(5k) are the lower-level problem that represents the distribution network pricing scheme in (4). The hacker aims to maximize system EV loads during peak hour period from time step t_0 to time step t_m, i.e. objective (5a). Since the traditional LRA model (3) is a bi-level optimization problem, we apply KKT conditions on (1a)-(1e) to get its dual problem. KKT conditions consists of four constraints: primal constraints, dual constraints, complementary slackness, and the stationary equation. $\widetilde{\lambda}^t$, $\sigma^+_{i,t}$, $\sigma^-_{i,t}$, $\pi^+_{j,t}$, $\pi^-_{j,t}$ are dual variables with respect to constraint (1c), (1e) and (1d) at time t. Constraints (5b), (1b) and (1d)-(1e) are the primary feasibility in the exact OPF problem. Note that since it takes time for EV users to react to the charging price change, in (5b) we use historical EV data to maintain consistency with the LRA model. Constraint (5c) is the dual feasibility to ensures that the dual variables with respect to inequalities are larger than zero. (5d)-(5g) are the complementary slackness form of (1d)-(1e). (5h) is the stationarity equation for (1). After the KKT condition transformation, the dual variable in (2) is successfully introduced. Therefore, we introduce the LMP to the LRA model just as shown in (5i).

By introducing optimization model (4) as the lower level problem in (5), a relationship between charging price and the LMP is built. We can infer from (4) that when the LMP on EV bus is decreased, the DNO will evaluate the price-demand constraint (4b) and determine the new charging price μ^t_k and charging demand $P^t_{EV_k}$. Therefore, LMP serves as the bridge between LRA and charging price to ensure that the attack can stimulate a EV demands increase. More parallel lower-level problem such as (5j)-(5k) can be attached to (5) if more distribution network is considered during the attack.

Solving the bi-level optimization model (5) is complicated since it has parameters related to the previous time step, such as constraint (5b) and (4b). Also, considering that the attack might be exposed at any time, a greedy algorithm is applied to determine the best-attacking vector $\Delta P^t_{L_i}$. Instead of solving (3) between time range t_0 to t_m at once, we iteratively solve the problem in only one time step to find its current local optimal solution. During time step t, the hacker set $t_0 = t$ and $t_m = t_0 + 1$ in (5a) and solve the optimization problem (3).

Therefore, the multi-slot problem is decompose into a single-step optimization problem. Since the DNO's operating cost $O(P_{EV_k}^t)$ in (5j) is a convex quadratic function with respect to EV load demand [19], the lower level problem (5i)-(5j) is convex. Assume that $O(P_{EV_k}^t) = b_0 P_{EV_k}^{t^2} + b_1 P_{EV_k}^t + b_2$ with $b_0 > 1/P_{EV_k}^{t_0,0} E^{t_0,t_0} \mu_k^{t_0,0}$, by solving the quadratic optimization problem (5j)-(5k), we can have the linear expression of (5k) under greedy algorithm:

$$P_{EV_k}^{t_0} = P_{EV_k}^{t_0,0}(1 + E^{t_0,t_0}(\mu_k^{t_0}/\mu_k^{t_0,0} - 1)) \tag{6a}$$

$$= P_{EV_k}^{t_0,0} E^{t_0,t_0} \mu_k^{t_0,0} (\lambda_k^{t_0} - b_1)/2(1 + b_0 P_{EV_k}^{t_0,0} E^{t_0,t_0} \mu_k^{t_0,0}). \tag{6b}$$

If the condition $b_0 > 1/P_{EV_k}^{t_0,0} E^{t_0,t_0} \mu_k^{t_0,0}$ fails, then the solution of quadratic optimization (5j)-(5k) must be at the boundary condition of $P_{EV_k}^t$. It is clear that when $P_{EV_k}^t = 0$, the profit of the DNO is zero. Therefore, the optimal solution can only be $P_{EV_k}^t = P_{EV_{max}}$.

Constraint (3e) is hard to solve since the binary variable $\delta_{L,i}^t$ and $\delta_{line,i}^t$ has no mathmatical representation. We use the following constraints to replace constraint (3e) [18].

$$\begin{cases} \Delta P_{L_i}^t + \tau P_{L_i}^{t-1} \delta_{L,i}^t \geq 0 \\ \Delta P_{L_i}^t - \tau P_{L_i}^{t-1} \delta_{L,i}^t < 0 \\ \delta_{L+,i}^t + \delta_{L-,i}^t - 2\delta_{L,i} \leq 0 \\ \Delta P_{L_i}^t + (-\tau P_{L_i}^{t-1} - \epsilon)\delta_{L+,i}^t \geq -\tau P_{L_i}^{t-1} \\ \Delta P_{L_i}^t + (\tau P_{L_i}^{t-1} + \epsilon)\delta_{L-,i}^t \leq \tau P_{L_i}^{t-1} \\ \delta_{L+,i}^t + \delta_{L-,i}^t + \delta_{L,i} < 2 \\ \delta_{L+,i}^t + \delta_{L-,i}^t - \delta_{L,i} \geq 0 \\ \delta_{L+,i}^t, \delta_{L-,i}^t, \delta_{L,i} \in \{0,1\} \end{cases} \forall i \in \mathcal{D} \tag{7}$$

$$\begin{cases} \Delta P_{line,i}^t + M\delta_{line,i}^t \geq 0 \\ \Delta P_{line_i}^t - M\delta_{line,i}^t < 0 \\ \delta_{line+,i}^t + \delta_{line-,i}^t - 2\delta_{line,i} \leq 0 \\ \Delta P_{line_i}^t + (-M - \epsilon)\delta_{line+,i}^t \geq -M \\ \Delta P_{line_i}^t + (M + \epsilon)\delta_{line-,i}^t \leq M \\ \delta_{line+,i}^t + \delta_{line-,i}^t + \delta_{line,i} < 2 \\ \delta_{line+,i}^t + \delta_{line-,i}^t - \delta_{line,i} \geq 0 \\ \delta_{line+,i}^t, \delta_{line-,i}^t, \delta_{line,i} \in \{0,1\} \end{cases} \forall i \in \mathcal{L} \tag{8}$$

Noted that M is a sufficiently large positive number and ϵ is a sufficiently small positive number. Binary variables $\delta_{L+,i}^t$, $\delta_{L-,i}^t$, $\delta_{line+,i}^t$, $\delta_{line-,i}^t$ are used to represent whether the attacking resources have reach their maximum or minimum limits. The existence of complementary slackness (5d)-(5g) makes the optimization nonconvex. A linearized expression of complementary slackness is applied to solve this problem [18].

$$\begin{cases} \pi_{i,t}^- \leq M\omega_{\pi_{i,t}}^- \\ P_{line,i}^t + P_{line,i}^{max} \leq M(1 - \omega_{\pi_{i,t}}^-) \\ \pi_{i,t}^+ \leq M\omega_{\pi_{i,t}}^+ \\ -P_{line,i}^t + P_{line,i}^{max} \leq M(1 - \omega_{\pi_{i,t}}^+) \\ \omega_{\pi_{i,t}}^- + \omega_{\pi_{i,t}}^+ \leq 1 \end{cases} \forall i \in \mathcal{L} \tag{9}$$

$$\begin{cases} \sigma_{i,t}^- \leq M\omega_{\sigma_{i,t}}^- \\ P_{G_i}^t - P_{G_i}^{min} \leq M(1 - \omega_{\sigma_{i,t}}^-) \\ \sigma_{i,t}^+ \leq M\omega_{\sigma_{i,t}}^+ \\ -P_{G_i}^t + P_{G_i}^{max} \leq M(1 - \omega_{\sigma_{i,t}}^+) \\ \omega_{\sigma_{i,t}}^- + \omega_{\sigma_{i,t}}^+ \leq 1 \end{cases} \forall i \in \mathcal{G} \tag{10}$$

$$\omega_{\sigma_{i,t}}^+, \omega_{\sigma_{i,t}}^-, \omega_{\pi_{i,t}}^+, \omega_{\pi_{i,t}}^- \in \{0,1\} \tag{11}$$

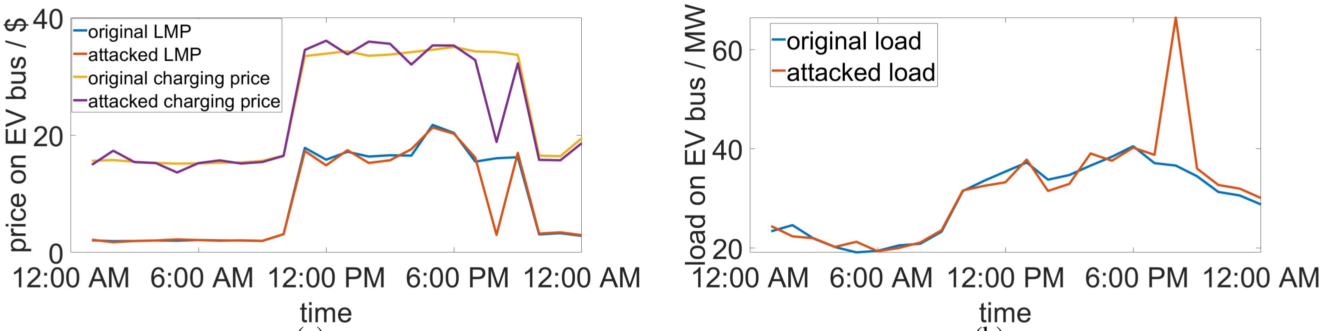
New binary varibles $\omega_{\sigma_{i,t}}^+, \omega_{\sigma_{i,t}}^-, \omega_{\pi_{i,t}}^+, \omega_{\pi_{i,t}}^-$ in equations (9), (10), (11) are used to represent whether the generators or branches have reached their maximum or minimum limits. By substituting (9), (10) and (11) to (5d)-(5g), the complementary slackness constraint become linear. Therefore, the problem becomes a mixed integer linear problem (MILP) in each step of the greedy algorithm, which can be solved numerically as shown in Algorithm 1.

Algorithm 1 Greedy algorithm for attack model

```
Input: Attack time range $t_0$, $t_m$
Output: Attack vector $\Delta P_{L_i}^t$
Initialize $t = t_0$
while $t \leq t_m$ do
    Estimate basic charging demand $P_{EV_k}^{t,0}$
    Estimate basic charging price $\mu_k^{t,0}$
    if $b_0 > 1/P_{EV_k}^{t,0} E^{t,t} \mu_k^{t,0}$ then
        Substitude (6a),(6b) to (5p)-(5r)
    else
        $P_{EV_k}^t = P_{EV_{max}}$
    Replace $t_0$ in (5a) with $t$
    Replace $t_m$ in (5a) with $t+1$
    Solve MILP problem (5)
    Output attack vector $\Delta P_{L_i}^t$
    if Attack is not exposed then
        $t = t + 1$
    else
        Break loop
return Attack vector $\Delta P_{L_i}^t$
```

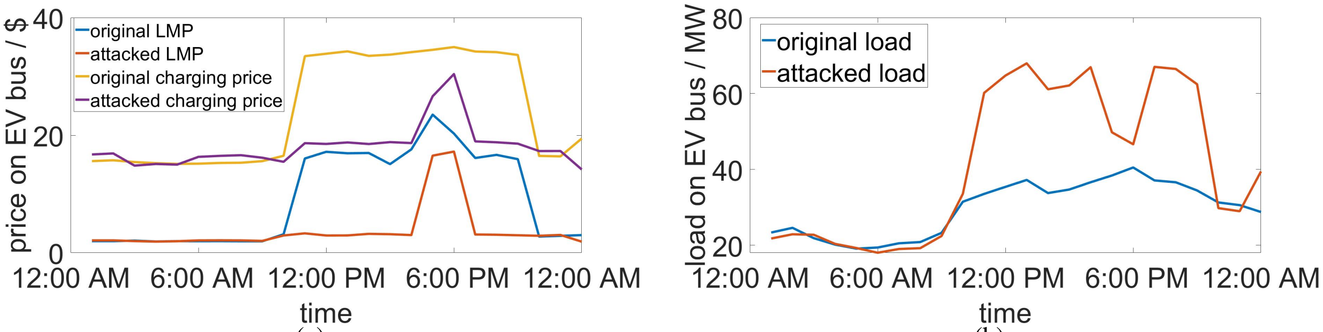
IV. Case Study

In this section, we apply our proposed attack method to the IEEE 30-bus system that consists of 6 generators, 24 load buses and 41 branches [23], [24]. A daily pattern of aggregated load data on June 21st, 2023 is taken from the Los Angeles Department of Water and Power electricity overview. We normalize the above data based on its maximum value and apply the pattern on the EV load bus. In the transmission network, bus-self admittance is ignored since we only consider active power demand. The maximum attack magnitude τ on each residential load bus is set to 50% of its original value [23]. The maximum attack resources is set as 80, which is about 75% of the total available measurement units. To simulate the measurement error and communication noise in reality, all the measurement data and hacker's attack vector is contaminated by independent Gaussian noises with $e \sim \mathcal{N}(0, 0.05)$ based on



(a) (b)

Fig. 3: (a) LMP, charging price, (b) load change on bus 12 under instant attack



(a) (b)

Fig. 4: (a) LMP, charging price, (b) load change on bus 12 under consecutive attack

its original value. Noted that the original LMP and charging price curve in this section is calculated without noise affect.

A. Attack on Single EV Bus

Bus 12 is set as an EV bus with around 10,000 EVs. Our attack aims to maximize the EV loads in EV buses. Because in the original LMP and the original charging price, the peak hours range from 11am to 11pm. Thus, we consider instant attacks at 8 pm and consecutive attacks from 11 am to 11 pm.

Fig. 3 gives the LMP, charging price, and EV load with and without the instant attack. As shown in Fig. 3(a), at 8 pm, the hacker successfully mislead the TNO to reduce the LMP on EV bus 12 and consequently cause a decrease in the charging price. EV users observe a sudden price decrease and all rush into charging at the same time, which results in a load increase from 37MW to 66MW as shown in Fig. 3(b). This indicates that our model works for an instant attack during peak hours.

Next, we expand the attacking period from 11 am to 11 pm, and launch the attack. Fig. 4 gives the LMP, charging price, and EV load with and without the consecutive attacks. It can be observed that the LMP almost remains unchanged under the attack during the peak hours. This indicates that the hacker successfully masks the congestion scenario in the transmission network and misleads the TNO about the LMP setting strategy. Since the LMP is almost unchanged, the DNO do not increase the charging price since it will reduce their profits as shown in Fig. 4(a). The EV load on bus 12 is therefore increased during the peak hour as shown in Fig. 4(b). Compared to the normal operation, the attack successfully increased the peak load from 40 MW to 68 MW, which indicates that our attack model effectively disturbs the price control scheme and create a load spike during peak hours.

B. Attack on Multiple EV Buses

In this section, we monitor the effectiveness of attacks on multiple EV buses. We set bus 12 as an EV bus with around 10,000 EVs and 1000 EVs on bus 27 since the original residential load on bus 27 is about 10% of the residential load on bus 12 in IEEE 30-bus model. We launch the consecutive attacks on both buses from 11 am to 11 pm. Fig. 5(a) shows the load change with and without attacks. We can observe that both EV loads on bus 12 and bus 27 increase during peak hours. EV load on bus 12 increased from 40MW to 60MW and EV load on bus 27 increased from 4MW to 8 MW. This indicates that our attack model also works on two EV buses.

To better testify the effectiveness of our model, we set bus 25 as an EV bus with 2500 EVs and monitored the load change among the whole system. The result of the EV load change is shown in Fig. 5(b). We can infer from Fig. 5(b) that the attack still works for three EV buses. The maximum load increment on bus 25 is 2.1MW, which is about 20% of its base value. The load on bus 12 is increased from 40MW to 62MW and the load on bus 27 is also increased by 80%.

As illustrated in the greedy algorithm, the hacker solves MILP problem (5) at each time interval. Therefore, the computational complexity of the proposed attack is determined by the total attacking time $t_m - t_0$ and the number of variables and constraints in (5). It is worth pointing out that only two linear constraints (5i) and (6) are added into the traditional LRA model [18]. The number of constraints in (5i) and (6) are the same as the number of EV buses. Therefore, the number

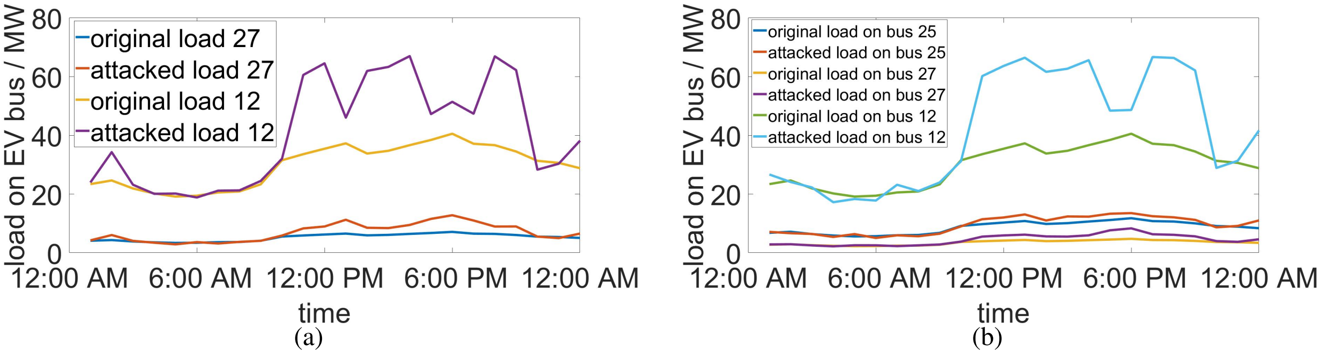


Fig. 5: load change on (a) bus 12 and 27 (b) bus 12,25 and 27 under consecutive attack

of constraints in (5) is linear to the number of EV buses in the system, which indicates that our algorithms can be easily extended to large systems with high EV penetration.

V. Conclusion and Future Challenge

In this paper, we have proposed a novel attack method that can trigger an EV load spike during peak hours. We apply the LRA in the transmission network to veil the congestion scenario and mislead the TNO to set the wrong LMP at EV buses. Consequently, the DNOs on EV buses do not increase the charging price in the retail market to get maximum profits. Therefore, the EV users charge simultaneously during peak hours and cause an EV load spike in the system. The case study in the IEEE 30-bus system proves the effectiveness of our attack model. We have carried out both an instant attack and consecutive attacks during the peak hour. Our simulations have shown that the proposed algorithm still performs effectively under multiple EV buses case. Considering that both residential and EV loads exist in practical distribution load buses, future research may be carried out in the optimization of different load combinations. Other multi-slot optimization algorithms can also be explored to reach a more stealthy and powerful attack in a high EV penetration network.

References

[1] D. S. Callaway and I. A. Hiskens, “Achieving controllability of electric loads,” *Proceedings of the IEEE*, vol. 99, no. 1, pp. 184–199, 2011.

[2] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, “False data injection on state estimation in power systems-attacks, impacts, and defense: A survey,” *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 411–423, 2017.

[3] S. Hussain, S. M. Hussain, M. Hemmati, A. Iqbal, R. Alammari, S. Zanero, E. Ragaini, and G. Gruosso, “A novel hybrid cybersecurity scheme against false data injection attacks in automated power systems,” *Protection and Control of Modern Power Systems*, vol. 8, no. 1, 2023.

[4] P. P. Kundur, N. J. Balu, and M. G. Lauby, *Power system stability and control*. The EPRI power system engineering series., New York: McGraw-Hill, 1994.

[5] D. Reeh, F. Cruz Tapia, Y. W. Chung, B. Khaki, C. Chu, and R. Gadh, “Vulnerability Analysis and Risk Assessment of EV Charging System under Cyber-Physical Threats,” *ITEC 2019 - 2019 IEEE Transportation Electrification Conference and Expo*, pp. 1–6, 2019.

[6] M. A. Sayed, R. Atallah, C. Assi, and M. Debbabi, “Electric vehicle attack impact on power grid operation,” *International Journal of Electrical Power and Energy Systems*, vol. 137, no. May 2021, p. 107784, 2022.

[7] S. Acharya, R. Mieth, R. Karri, and Y. Dvorkin, “False data injection attacks on data markets for electric vehicle charging stations,” *Advances in Applied Energy*, vol. 7, no. May, p. 100098, 2022.

[8] P. Jaruwatanachai, Y. Sukamongkol, and T. Samanchuen, “Predicting and Managing EV Charging Demand on Electrical Grids: A Simulation-Based Approach,” *Energies*, vol. 16, no. 8, pp. 1–22, 2023.

[9] N. Y. Soltani, S. J. Kim, and G. B. Giannakis, “Real-Time Load Elasticity Tracking and Pricing for Electric Vehicle Charging,” *IEEE Transactions on Smart Grid*, vol. 6, no. 3, pp. 1303–1313, 2015.

[10] C. H. Dharmakeerthi, N. Mithulananthan, and T. K. Saha, “Impact of electric vehicle fast charging on power system voltage stability,” *International Journal of Electrical Power and Energy Systems*, vol. 57, pp. 241–249, 2014.

[11] H. T. Reda, A. Anwar, and A. Mahmood, “Comprehensive survey and taxonomies of false data injection attacks in smart grids: attack models, targets, and impacts,” *Renewable and Sustainable Energy Reviews*, vol. 163, no. April, p. 112423, 2022.

[12] H. Li and Z. Han, “Manipulating the electricity power market via jamming the price signaling in smart grid,” *2011 IEEE GLOBECOM Workshops, GC Wkshps 2011*, pp. 1168–1172, 2011.

[13] L. Jia, R. J. Thomas, and L. Tong, “Malicious data attack on real-time electricity market,” *IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, pp. 5952–5955, 2011.

[14] L. Xie, Y. Mo, and B. Sinopoli, “False Data Injection Attacks in Electricity Markets,” *2010 First IEEE International Conference on Smart Grid Communications*, pp. 226–231, 2010.

[15] A. Tajer, “False Data Injection Attacks in Electricity Markets by Limited Adversaries: Stochastic Robustness,” *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 128–138, 2019.

[16] S. Bi and Y. J. Zhang, “False-data injection attack to control real-time price in electricity market,” *GLOBECOM - IEEE Global Telecommunications Conference*, pp. 772–777, 2013.

[17] Y. Wang, C. Chen, S. Zhang, Y. Liu, C. Huang, and Y. Du, “A tri-level programming-based frequency regulation market equilibrium under cyber attacks,” *Protection and Control of Modern Power Systems*, vol. 8, no. 1, 2023.

[18] Y. Yuan, Z. Li, and K. Ren, “Modeling load redistribution attacks in power systems,” *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 382–390, 2011.

[19] K. Feng, H. Zhou, Z. W. Liu, and D. Hu, “Retail market pricing design in smart distribution networks considering wholesale market price uncertainty,” *Proceedings IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society*, vol. 2017-Janua, pp. 5968–5973, 2017.

[20] L. Gong, W. Cao, K. Liu, Y. Yu, and J. Zhao, “Demand responsive charging strategy of electric vehicles to mitigate the volatility of renewable energy sources,” *Renewable Energy*, vol. 156, pp. 665–676, 2020.

[21] H. Yang, X. He, S. Member, Z. Wang, G. S. Member, R. C. Qiu, Q. Ai, and S. Member, “Blind false data injection attacks against state estimation based on matrix reconstruction,” *IEEE Transactions on Smart Grid*, vol. 13, no. 4, pp. 3174–3187, 2022.

[22] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” *ACM Transactions on Information and System Security*, vol. 14, no. 1, 2011.

[23] J. Yan, B. Tang, and H. He, “Detection of false data attacks in smart grid with supervised learning,” *Proceedings of the International Joint Conference on Neural Networks*, vol. 2016-Octob, pp. 1395–1402, 2016.

[24] G. Cheng, Y. Lin, J. Zhao, and J. Yan, “A Highly Discriminative Detector Against False Data Injection Attacks in AC State Estimation,” *IEEE Transactions on Smart Grid*, vol. 13, no. 3, pp. 2318–2330, 2022.